



The Desktop Resource for the Joint Clearance and Access Verification System (JCAVS)

**A Subsystem of the
Joint Personnel
Adjudication System
(JPAS)**

Aug 2006

The Desktop Resource for the Joint Clearance & Access Verification System (JCAVS)

A Subsystem of the Joint Personnel Adjudication System (JPAS)

IMPORTANT NOTICE TO JPAS USERS: The Defense Security Service provides the JPAS application for use by all services and agencies throughout the Department of Defense. JPAS functionality is designed to complement the Department's Personnel Security Program. Users should be mindful that self-help tools such as Frequently Asked Questions (FAQ), training tools and the JCAVS Desktop Resource provide guidance to the functionality of JPAS and should not be confused with Department, Agency or Service Policy. Users must refer to their agency policy whenever there is a conflict between policy and these self-help tools. Users should direct questions of policy to their personnel security program authority or contact their JPAS Program Functional Manager.

(Aug 2006)

Introduction

The Joint Personnel Adjudication System (JPAS) represents a major technological leap for Department of Defense (DoD) personnel security professionals worldwide. It is a DoD system that will use the Web to connect security personnel around the world with a database managed by DoD Agency Central Adjudication Facilities (CAF).

JPAS is the Department of Defense (DoD) personnel security migration system:

- providing the virtual consolidation of the DoD Central Adjudication Facilities (CAF)
- for use by non-SCI security program managers, Special Security Officers, Special Access Program (SAP) program managers, and DoD contractor security officers
- that will use a centralized database with centralized computer processing and application programs for standardized DoD personnel security processes.

JPAS provides "real-time" information regarding clearance, access and investigative status to authorized DoD security personnel and other interfacing organizations such as the Defense Security Service, Defense Manpower Data Center, Defense Civilian Personnel Management System, Office of Personnel Management, and Air Force Personnel Center.

JPAS is comprised of two major subsystems, the Joint Adjudication Management System (JAMS) and the Joint Clearance and Access Verification System (JCAVS).

JPAS = JAMS + JCAVS

JAMS provides Central Adjudication Facilities (CAFs) a single information system to assist in the adjudication process and standardizes core DoD Adjudication processes. JAMS is used by adjudicators to record eligibility determinations and command access decisions, and promotes reciprocity between the DoD CAFs.

JCAVS provides security personnel the ability to constantly update clearance and access information in real time to ensure that the most current clearance information is available throughout DoD. JCAVS promotes interoperability/interconnectivity with the following information systems:

- Defense Security Service (DSS)
- Office of Personnel Management (OPM)
- Defense Enrollment Eligibility Reporting System (DEERS)
- Defense Civilian Personnel Management System (DCPMS)
- Air Force Personnel Center (AFPC)
- DoD CRIM/IG (investigative data)
- Defense Finance Accounting System (DFAS)

The advent of JPAS creates the necessity for change to our current terminology. Currently we use such terms as “security clearance.” JPAS will speak in terms of eligibility and access instead of personnel security clearance. It will remain the government’s responsibility to issue eligibility to an individual, but only the security officer can assign one’s access level in JCAVS.

JCAVS uses “User Levels” to control functionality and the information displayed. The users of each level, functionality and eligibility requirement are defined as:

- **LEVEL 2** – Sensitive Compartmented Information (SCI) security personnel at unified command, DoD agency, military department or major command/equivalent headquarters. For industry, usually the Chief Security Officer at the corporate level, Special Security Officer (SSO) or Contractor Special Security Officer (CSSO). Provides Read and Write Access.
- **LEVEL 3** – SCI security personnel subordinate to Level 2 at a particular geographic location (installation, base, post, naval vessel or facility). Provides Read and Write Access.
- **LEVEL 4** – Non-SCI security personnel at unified command, DoD agency, military department or major command/equivalent headquarters. For industry, corporate FSOs (non-SCI). Provides Read and Write Access.
- **LEVEL 5** – Non-SCI security personnel subordinate to Level 4 at a particular geographic location (installation, base, post, and naval vessel). For industry Company FSOs / Managers (non-SCI). Provides Read and Write Access.
- **LEVEL 6** – Unit security manager (additional duty) responsible for security functions as determined by responsible senior security official. For industry, Unit Security Managers / Visitor Control. Provides Read and Write Access.
- **LEVEL 7** – Non-SCI Entry control personnel. Individuals who grant access to installations, buildings, etc. For industry, lobby receptionists, security entry point personnel (non-SCI). Provides Read Only Access.
- **LEVEL 8** – SCI Entry control personnel. Individuals who grant access to Sensitive Compartmented Information Facility (SCIF) installations, buildings, etc. For industry, lobby receptionists, security entry point (SCI). Provides Read Only Access.
- **LEVEL 10** – Visitor Management. Level 10 users will have the same view of the JCAVS Person Summary as a JCAVS Level 7 User. They will receive Visit Notifications when their Security Management Office (SMO) is being notified of a visit. A Level 10 User may **not** be an Account Manager, create or delete an account at any level.

Each level has a requirement for an investigation and eligibility. SCI levels require access. For particular investigation and eligibility as they pertain to account levels, contact your Account manager, functional representative or the DoD Security Services Center for guidance.

NOTE: The term non-SCI refers to collateral information.

Remember: This Desktop Resource addresses instructions on the use of the JCAVS. It is an instructional tool only and is not meant to dictate policy.

For additional questions, clarification and/or points of contact, please see the JPAS website:

[HTTPS://jpas.dsis.dod.mil](https://jpas.dsis.dod.mil)

or

[HTTPS://diss.dsis.dod.mil/portal/appmanager/gateway/diss](https://diss.dsis.dod.mil/portal/appmanager/gateway/diss)

Screen shots used are for demonstration purposes only.

(Names may not match throughout each scenario.)

The Table of Contents

	<i><u>Page</u></i>
<u>Introduction</u>	1
 <u>Sections</u>	
1. Login	6
2. How to Lookup a Record	14
3. Account Manager Functions	17
4. How to Establish a Personnel Security Management Network (PSM Net)..	28
5. How to Add a Record.	34
6. How to Add a Category	36
7. How to In-Process	40
8. How to Indoctrinate	
a. Non-Sensitive Compartmented Information (Non-SCI)	42
b. SCI	46
9. How to Debrief	
a. Non-Sensitive Compartmented Information (Non-SCI)	50
b. SCI	53
10. How to Out-Process (Removal from PSM Net).	56
11. How to Enter a Separation Date	61
12. How to Document “PSQ Sent”	64
13. JCAVS Interface with E-QIP.	66
a. How do you get permission to use the JCAVS interface with e-QIP? ...	67
b. Other Pre-requisites	68
c. How do you initiate an investigation in JCAVS	69
d. What are the timelines when initiating, reviewing and approving an e-QIP submission?	75
e. How to Review and Approve an e-QIP submission	76
f. Process	76
g. Review	77
h. Approve	80
i. Revise	82

j. Stop	83
k. Where do I mail release forms?	84
l. What about the Applicant?	85
14. How to Generate a Request to Research/Upgrade Eligibility (RRU)	86
15. How to Check Notifications	88
16. How to Generate A Report	92
17. Mass Personnel Changes (Industry)	97
18. Terms & Definitions	101
19. Acronyms	102
20. Index of Figures	104

Section 1 - Login

Logging On to JPAS

To log onto JPAS:

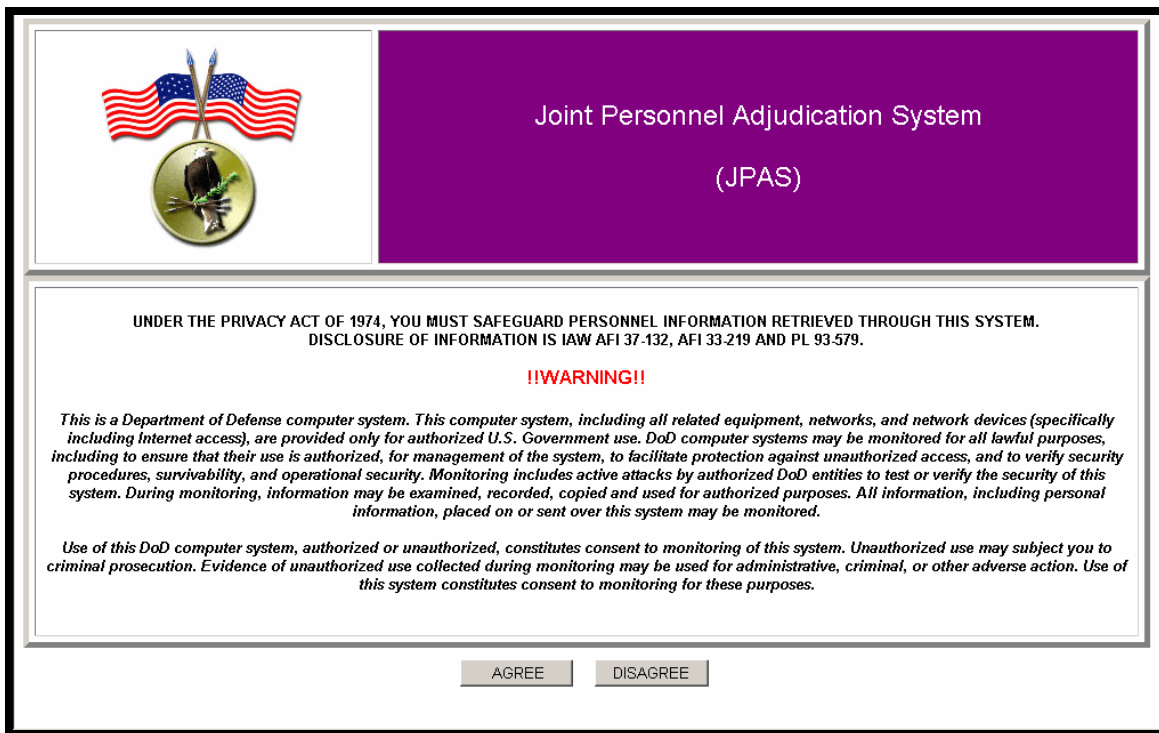
1. Open your browser and enter the address of the JPAS Gateway home page, <https://jpas.dsis.dod.mil/>, in the address window. Press **Enter**. The JPAS Gateway home page appears (Figure 1).

Figure 1: JPAS Gateway Home Page



2. Click the **JPAS LOGIN** link on the left side of the home page. The JPAS disclosure screen appears (Figure 2).

Figure 2: JPAS Disclosure Screen



The JPAS Disclosure Screen is a web-based interface. At the top left, there is a circular emblem featuring two crossed flags (one American, one green) and a globe. To the right of this emblem is a large purple rectangular box containing the text "Joint Personnel Adjudication System (JPAS)" in white. Below the purple box, the screen displays a privacy notice in black text, followed by a red "!!WARNING!!" heading. The notice details the Department of Defense's monitoring policies. At the bottom, there are two buttons: "AGREE" and "DISAGREE".

Joint Personnel Adjudication System
(JPAS)

UNDER THE PRIVACY ACT OF 1974, YOU MUST SAFEGUARD PERSONNEL INFORMATION RETRIEVED THROUGH THIS SYSTEM.
DISCLOSURE OF INFORMATION IS IAW AFI 37-132, AFI 33-219 AND PL 93-579.

!!WARNING!!

This is a Department of Defense computer system. This computer system, including all related equipment, networks, and network devices (specifically including Internet access), are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored.

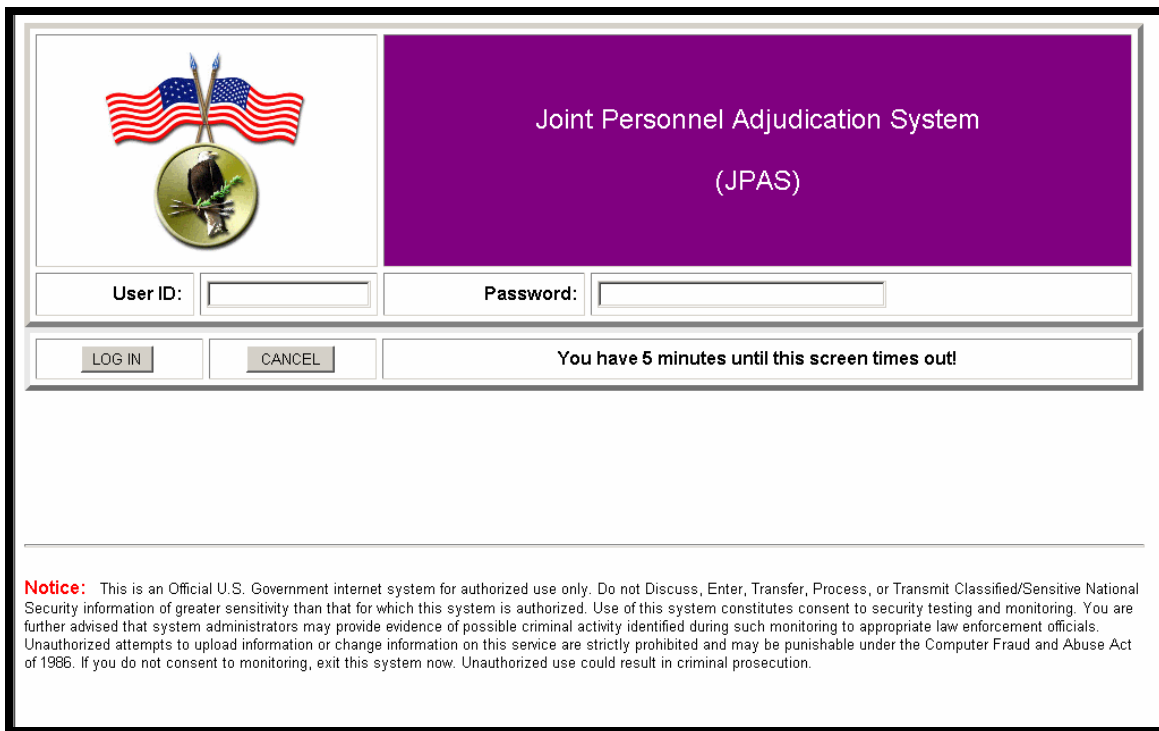
Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

AGREE DISAGREE

NOTE: The JPAS disclosure screen contains a message reminding you that JPAS is a highly secure system available only to authorized users. You must agree to all of the requirements stated in this message in order to gain access to the system. To consent to these requirements and proceed to the next step, select the **AGREE** button. If you are unable to comply with these requirements for any reason, select the **DISAGREE** button.

3. Click **AGREE**. The JPAS log in screen appears (Figure 3).

Figure 3: JPAS Log In Screen



The JPAS Log In Screen features a header with the Joint Personnel Adjudication System (JPAS) logo on the left and the system name on a purple background on the right. Below the header are input fields for User ID and Password, each with a 'LOG IN' button. A 'CANCEL' button is also present. A timer indicates 'You have 5 minutes until this screen times out!'. A 'Notice' section at the bottom provides legal disclaimers regarding the system's use and security.

Joint Personnel Adjudication System
(JPAS)

User ID: Password:

LOG IN CANCEL

You have 5 minutes until this screen times out!

Notice: This is an Official U.S. Government internet system for authorized use only. Do not Discuss, Enter, Transfer, Process, or Transmit Classified/Sensitive National Security information of greater sensitivity than that for which this system is authorized. Use of this system constitutes consent to security testing and monitoring. You are further advised that system administrators may provide evidence of possible criminal activity identified during such monitoring to appropriate law enforcement officials. Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986. If you do not consent to monitoring, exit this system now. Unauthorized use could result in criminal prosecution.

4. Type your **User ID** and **Password** in the appropriate text boxes. Remember that User ID and Passwords are case-sensitive.
5. Click **LOG IN**. The Choose Category/Level screen appears (Figure 4).

NOTE: Your eligibility and investigation are validated when you log onto the system. If you do not meet the necessary requirements, you will not be granted access to the system.

NOTE: A *Password Expired* message will appear the first time you log onto the system. Click **OK** and complete the steps described under **Creating a Permanent Password** below. If you already have a permanent password, skip to **Choosing Category/Level** on the next page.

Creating a Permanent Password

When your user account was created, the system automatically generated a temporary password for you. If this is the first time that you are logging onto the system, enter the **User ID** and temporary **Password** that has been given to you by the account manager who created your account. When you see the *Password Expired* message, select **OK** to open the **Change Password** dialog box. Here you must change the temporary password to a permanent one of your choice. Please follow these guidelines in creating your new password:

- Passwords are case-sensitive.
- Passwords must be between 10 and 20 characters in length.
- Passwords must contain at least two different lowercase letters, two different uppercase letters, two different numbers, and two different special characters.
- The new password can not be the same as any of the previous 10 passwords.
- The new password can not be any password used in the previous 18 months.

Once you have entered your new, permanent password, follow the prompts to confirm your new password and proceed to the next step. Be sure to protect the security of your password according to the policies of your organization.

Choosing a Category/Level

The JCAVS Choose Category/Level screen (Figure 4) is where you select the category or level that has been assigned to you. Your assigned level and category determine the menu options available to you.

NOTE: If you are assigned to a single Person Category and a single Level, the Welcome screen and Main Menu appear instead.

Table 1 identifies JCAVS levels and their associated functions and responsibilities.

Table 1: JCAVS Levels, Functions, and Responsibilities

Levels	Functions/Titles
Account Manager	Add, Modify, and Remove JCAVS user
Levels 2 and 3	SCI Personnel Security Professionals
Levels 4 and 5	Non-SCI Personnel Security Professionals
Level 6	Unit Security Manager
Level 7 (Read only)	Entry Control Personnel (Non-SCI)
Level 8 (Read only)	Entry Controller (SCI)
Level 10 (Visits only)	Visitor Control

Figure 4: Choose Category/Level screen

The screenshot shows a Netscape browser window titled "JPAS Choose Category/Role - Netscape". The address bar displays "https://204.230.206.200/JPAS/servlets/com.eds.jpas.client.servlets.JPASLoginServlet". The main content area has a heading "Choose Category/Level" in purple. Below the heading, there is a form with the following fields:

- User ID:** artmasq
- Person Category:** C - Active Duty (dropdown menu)
- Level:** Account Manager (dropdown menu)
- OK** button

At the bottom of the form, there is a **Notice:** Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

To choose a category and level:

1. Click the **Person Category** drop-down arrow and select your category.
2. Click the **Level** drop-down arrow and select your user level.

NOTE: Select **Account Manager** to create/update/deactivate a Security Management Office (SMO); add, modify, remove, log off, lock or unlock another user's account; or reset a user's password.

3. Click **OK**. The Welcome screen and Main Menu appear (Figure 5).

Note: The Welcome screen will display the last successful and unsuccessful logon time and date

JCAVS Welcome Screen and Main Menu

The JCAVS Welcome screen and Main Menu indicates you have successfully logged into JCAVS.

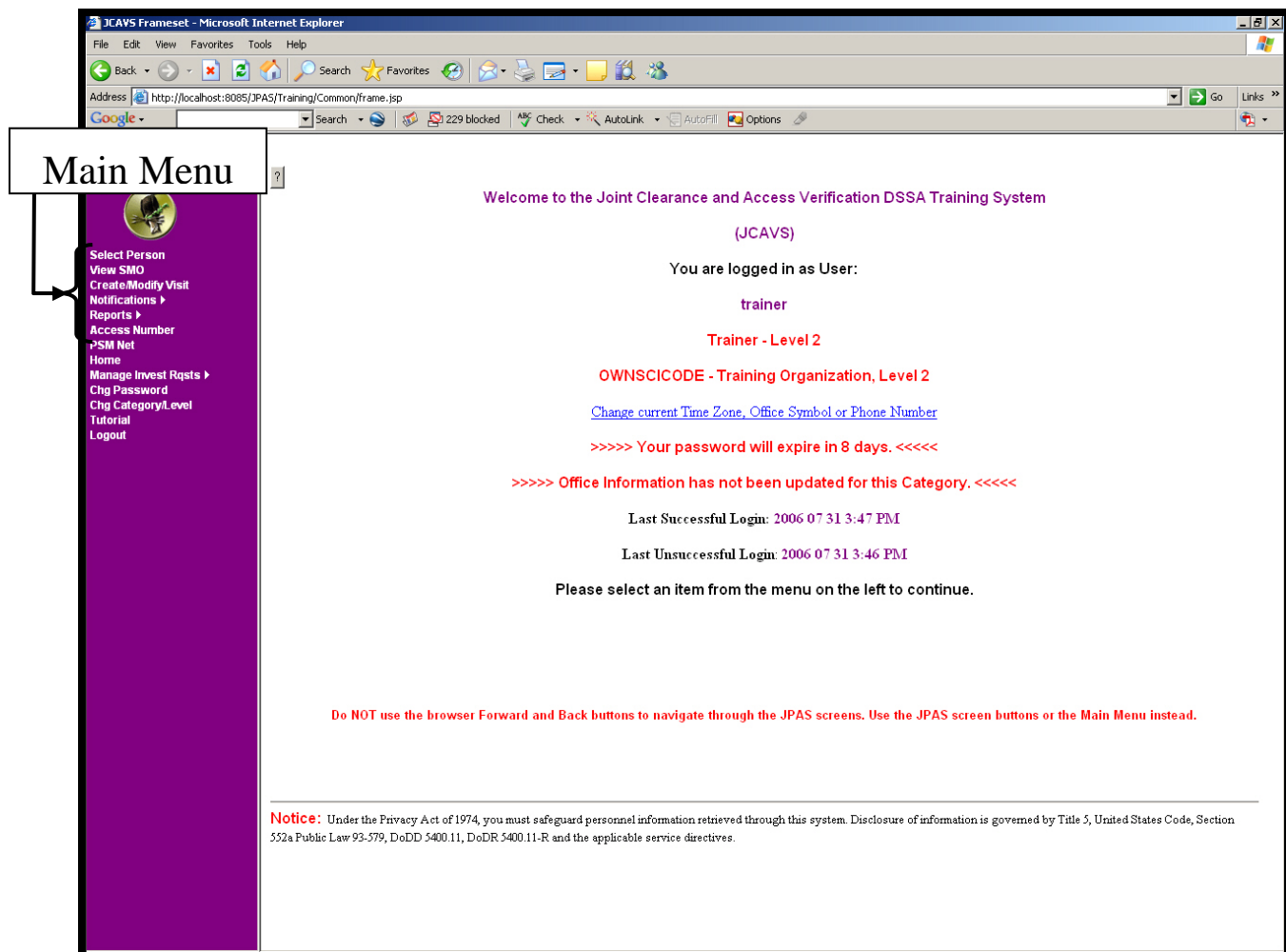
Welcome Screen

Your user ID and access level are displayed on the Welcome screen. The Welcome screen will also display the last successful and unsuccessful logon time and date

Main Menu

From the Main Menu, you can navigate to different system functions using the options listed on the Main Menu displayed to the left of the Welcome screen.

Figure 5: JCAVS Welcome screen and Main Menu



Office Information

You can change or update office information for a user's Person Category by selecting the **Change current Time Zone, Office Symbol or Phone Number** link located in the middle of the Welcome screen.

Entering Office Information

To enter office information:

6. Click on the **Change current Time Zone, Office Symbol or Phone Number** link. The Change Office Symbol/Telephone Number/Time Zone screen appears (Figure 6).
7. If applicable, type the new office symbol in the **New Office Symbol** text box.
8. From the **User's Current Time Zone** drop-down list select the correct **Time Zone**. The **Current Time Zone** is automatically populated with the selected time zone.
9. Type the appropriate information in the text boxes across the **Commercial** row under the headings: **Country Code**, **Area Code**, **Prefix and Exchange**, and **Extension**.
10. If applicable, type the appropriate information in the text boxes across the **DSN** row under the headings **Country Code**, and **Prefix and Exchange**.
11. Click **Save**. The JCAVS Welcome screen and Main Menu appears.

Figure 6: Change Office Symbol/Telephone Number/Time Zone screen

The screenshot shows a Netscape browser window titled "JCAVS Main Screen - Netscape". The address bar displays the URL: <https://204.230.206.200/JPAS/servlets/com.eds.ipas.client.servlets.JPASChooseRoleServlet>. The page title is "Change Office Symbol/Telephone Number/Time Zone".

The form displays user information: **BENSON, JOSEPH T**, **SSN:** [redacted], **Grade:** O3, and **Category:** Active Duty - Officer (USAF).

The form includes the following fields and sections:

- *New Office Symbol:** CCJ2
- *User's Current Time Zone:** [dropdown menu]
- Enter New Phone Numbers Below:**
 - *Commercial:** [Country Code:], [Area Code:], [Prefix and Exchange:], [Extension:]
 - DSN:** [Country Code:], [Prefix and Exchange: 8284967]
- Buttons:** SAVE, CANCEL

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

Intentionally left blank

Section 2 – How to Lookup a Record

Introduction

JPAS was developed so that a person's eligibility, access, and investigation type could be verified. Within JPAS, you will be able to lookup anyone's record and determine whether or not they have a current eligibility as long as you have their Social Security Number (SSN).

NOTE: JPAS was not designed to lookup a person's eligibility prior to hiring. You cannot use JPAS for any part of the personnel hiring process.

Instructions

1. Log in as a **User**.
2. Click on **Select Person** (column on left) to display the Select Person screen (Figure 7).

Figure 7: Select Person screen

Select Person

*SSN:

Last Name:

First Name:

Middle Name:

Display Person Summary: ☒

Display abbrev. Person Summary with VISIT Info: ☐

Display Add/Modify Non-DoD Person: ☐

Display SII: ☐

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

3. Enter the person's **SSN**.
4. **Select** the **Display Person Summary** radio button.
5. Click the gray **Display** button to display the Person Summary screen (Figure8).

Figure 8: Person Summary screen

Person Summary

RED, ERIC A
Person Category

Active Duty - Enlisted (USAF)

SSN: 995-82-6810
Open Investigation: N/A
PSQ Sent Date: N/A
Attestation Date: 1999 06 18
Incident Report: N/A
SF 713 Fin Consent Date: N/A
SF 714 Fin Disclosure Date: N/A
Polygraph: N/A
Foreign Relation: N/A

Date of Birth: 1972 07 22
Marital Status: N/A
Place of Birth: Maine
Citizenship: U.S. Citizen
NdA Signed: Yes
NdS Signed: Yes

Accesses

Category	US Access	NATO Access	PSP	Suitability and Trustworthiness	SCI
Active Duty - Enlisted (USAF)	Top Secret	NATO S	No	IT: N/A Public Trust: N/A Child Care: N/A	SI TK G HCS

[Access Number: N/A](#)

Person Category Information

Category Classification: N/A
Organization: EEOUFHGC, 25 INFO OPNS SQ, Hurlburt Field, Hurlburt Field, FL, 32544
Organization Status: N/A
Occupation Code: K1A851E
SCI SMO: N/A
Non-SCI SMO: N/A
Serving SMO: Yes
Office Symbol: DOT
Position Code: N/A
Arrival Date: 2002 10 09
Office Phone Comm: N/A
Separation Status: N/A
Interim: N/A

Separation Date: 2007 01 11
Grade: E6
PS: N/A
RNLTID: N/A
Office Phone DSN: N/A
TAFMSD: 1992 05 26
Proj. Departure Date: N/A
Proj. UIC/RUC/PASCODE: N/A

[Report Incident](#)
[In/Out Process](#)

Investigation Summary

SBPR from DSS, Opened: 1999 12 28 Closed 2001 03 20
SSBI from DSS, Opened: 1992 12 23 Closed 1992 12 23

Adjudication Summary

PSI Adjudication of SBPR DSS, Opened 1999 12 28, Closed 2001 03 20, determined Eligibility of SCI - DCID 6/4 on 2001 05 22
AFCAF
PSI Adjudication of SBPR DSS, Opened 1999 12 28, Closed 2001 03 20, determined Eligibility of SCI - DCID 6/4 on 2001 05 22
AFCAF

External Interfaces

[Perform SII Search](#)
[DCII](#)

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

- The person's Person Summary screen should appear with the person's name printed at the top.

7. The Personal Identification Data section of the Person Summary screen will display the **Person Category** drop down menu and other fields such as **SSN, Date of Birth ,Open Investigation, Marital Status, PSQ Sent Date, Place of Birth, Attestation Date, Citizenship, and Incident Report.** (This is not an all inclusive list.)
8. The second section of the Person Summary screen called the **Accesses** Section will display access information that is presented in columns by Person Category. If no information exists for any Person Category, the column does not display. Under this section you will normally see 4 columns: **Category, PSP, Suitability and Trustworthiness and SCI.** If you have a PSM Net relationship and the member meets requirements for indoctrination, you will see an **Available Action** column.
9. The third section of the Person Summary screen, called the **Person Category Information** section, will appear only if an individual has a Person Category. Information displayed is based on the category selection made in the Personal Identification Data section. Some of the types of information you will see when you change a category are: the Organization assigned to that category, the non-SCI SMO and/or the SCI SMO for that category, Separation status, etc. If you're updating information in this section, ensure the correct category is selected in the Personal Identification Data Section.
10. At the bottom of the Person Summary screen, you will find the **Investigation Summary,** the **Adjudication Summary** and the **External Interfaces** sections.
11. To get out of the Person Summary screen, you will have to make a new selection from the main menu.

Section 3 - Account Manager Functions

Maintaining a Security Management Office

PSM Net is based on security relationships with individual Person Categories instead of units or organizations. A Security Management Office (SMO) is associated with the personnel for whom the Person Categories have responsibility.

Creating a Security Management Office

1. On the Main Menu, click on the **Maintain Security Management Office** link. The Security Management Office Search screen appears (Figure 9).

Figure 9: Security Management Office Search screen

Security Management Office Search

*Enter Search Criteria:

Code:

Name:

Location:

Records 1 - 1 of 1, Page 1 of 1

Click on Code link below in order to select SMO

SMO Code	SMO Name	SMO Location
CB0003	AU1LFCMQ 0089 SECURITY FORCES SQ, Level 2	ANDREWS AFB, MD

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

2. Enter the SMO Code for your organization in the **Code** text box and click **Add**. (This option is not shown in Figure 9).
3. The Security Management Office Maintenance screen appears with a message window directing you to enter the required fields to add to the SMO (Figure 10).

Figure 10: Security Management Office Maintenance screen

Security Management Office Maintenance

*SMO Code: 123XXX
 *SMO Name:
 *SMO Location:
 *Service/Agency: DD - Department of Defense
 *Office Level:
 *Active Date: Deactivate Date: Deactivate: ☐
 *Commercial Phone: Commercial Fax: DSN Phone:
 Email:
 "B" Designation: ☐ NRO Designation: ☐ Service Secretary Designation: ☐
 Polygraph Designation: ☐ OSD/ES Designation: ☐

Active Parent SMO(s)

Code	Name	Relationship	Level	Begin Date	End Date
<div> <div>View</div> <div>Save</div> <div>Delete</div> <div>Cancel</div> </div>					

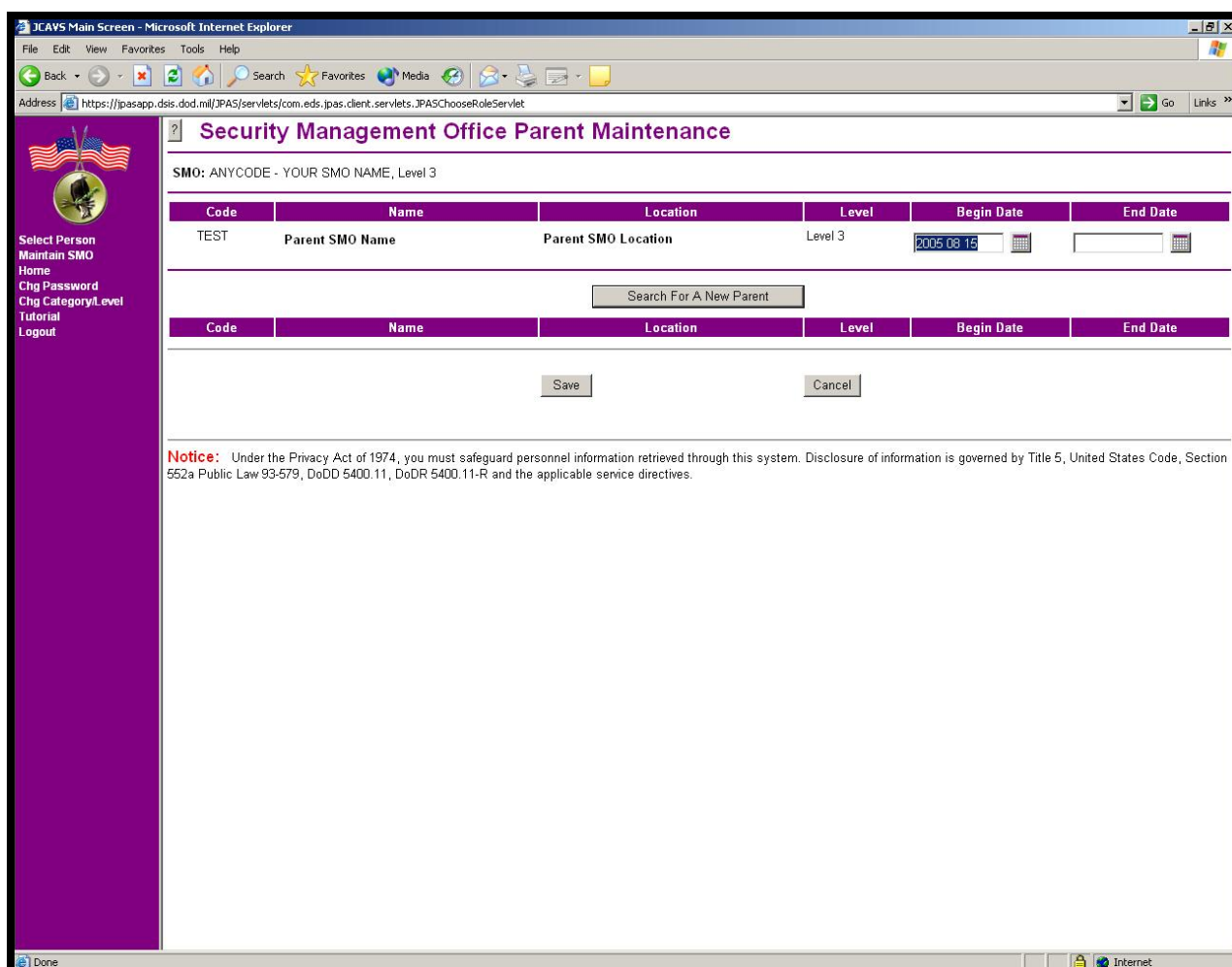
Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

4. Click **OK**.
 5. Type the SMO name in the **SMO Name** text box.
 6. Type the location of the SMO in the **SMO Location** text box.
 7. Click on the **Service/Agency** down arrow and select the appropriate service or agency.
 8. Click on the **Office Level** down arrow and select the appropriate level.
 9. Type the appropriate date in the **Active Date** text box.
 10. Type the commercial phone number in the **Commercial Phone** text box.
 11. Type the commercial fax number in the **Commercial Fax** text box.
 12. Type the DSN Phone number in the **DSN Phone** text box.
 13. Type in the email address in the **Email** text box.
 14. If applicable, click the appropriate **Designation**.
- To add a parent relationship, complete steps 15-21:

15. Click **Save**. The SMO is created and the screen refreshes.

16. Click on the **Add/Maintain Parent Relationships** button. The Security Management Office Parent Maintenance screen appears (Figure 11).
17. Click the **Search For A New Parent** button. The Security Management Office Search screen appears (Figure 9).
18. Type your SMO Code in the **Code** text box and click **Search**.
19. Click the appropriate SMO Code from the **SMO Code** list. The Security Management Office Parent Maintenance screen reappears (Figure 11).
20. Type in the appropriate date (Format: YYYY MM DD) in the **Begin Date** text box. If applicable, type the appropriate end date in the **End Date** text box.
21. Click **Save**. The Security Management Office Parent Maintenance screen is refreshed with the parent organization added to the upper portion of the screen.

Figure 11: Security Management Office Parent Maintenance screen



JCAVS Main Screen - Microsoft Internet Explorer

Address: https://jpasapp.ds.is.dod.mil/jPAS/servlets/com.eds.jpas.client.servlets.JPASChooseRoleServlet

Security Management Office Parent Maintenance

SMO: ANYCODE - YOUR SMO NAME, Level 3

Code	Name	Location	Level	Begin Date	End Date
TEST	Parent SMO Name	Parent SMO Location	Level 3	2005 08 15	

Search For A New Parent

Code	Name	Location	Level	Begin Date	End Date
------	------	----------	-------	------------	----------

Save Cancel

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

Updating a Security Management Office

1. On the Main Menu, click **Maintain Security Management Office**. The Security Management Office Search screen appears (Figure 9).
2. Type the SMO Code in the **Code** text box and click **Search**. The screen refreshes and displays a list of all Security Management Offices that matches the search query.
3. Click the **link** for the code that matches the SMO. The Security Management Office Maintenance screen for the selected SMO Code appears.
4. Update the necessary data.
5. Click **Save**. The Security Management Office Maintenance screen refreshes with updated data.

Deactivating a Security Management Office

1. Click **Maintain Security Management Office Search** on the Main Menu. The Security Management Office Search screen appears (Figure 9).
2. Type the SMO Code of the Security Management Office to be deactivated in the **Code** text box and click **Search**. The screen refreshes and displays a list of all Security Management Offices that match the search query.
3. Click on the **link** for the code that matches the appropriate Security Management Office. The Security Management Office Maintenance screen appears (Figure 11).
4. Click on the **check box** next to **Deactivate**.
5. Click **Save**. A message regarding the SMO update is displayed. Click **OK**. The SMO is deactivated and the deactivation date is displayed.

User Maintenance

The Select Person screen (Figure 7) allows you to select the record of an individual from within the application.

Selecting a Person

The recommended way to select a record is for the user to type in the individual's Social Security Number (SSN) and click the **DISPLAY** button. The SSN is compared to all records in the database until a match is found. The Person Summary screen (Figure 8) will appear with the data associated to the individual.

To select the person whose data you need to access:

1. On the Main Menu, click **Select Person**. The Select Person screen appears (Figure 7).
2. Type the **SSN** of the person whose record you want to view and click **Display**. The Add/Modify/Remove JCAVS User screen appears (Figures 12a and b).

Adding, Modifying, or Removing a JCAVS User's Account

The Add/Modify/Remove JCAVS User screen (Figures 12a and b) allows Account Managers to add and modify JCAVS user levels, or remove a JCAVS User ID from the JPAS system. Account Managers can assign the user's level and identify any special privileges or permissions (e-QIP) that apply to the user. The screen also allows the account manager to reset user passwords, lock and unlock accounts, and log users out of the application.

Figure 12a: Add/Modify/Remove JCAVS User screen

The screenshot shows a Netscape browser window titled "JCAVS Main Screen - Netscape". The address bar displays "https://204.230.206.200/JPAS/servlets/com.eds.jpas.client.servlets.JPASChooseRoleServlet". The main content area is titled "Add/Modify/Remove JCAVS User" and displays information for "KELLER, RICHARD LANCE". The SSN field is empty, and the UserID field is also empty. The Category is set to "Active Duty (USA)" and the Grade is "E05". Below this, there are sections for "Unauthorized User Level(s)" and "Authorized User Level(s)". The Unauthorized section shows a table with columns "Level" and "SMO", containing one row with "Level" and "SMO". The Authorized section shows a table with columns "Level" and "SMO", containing one row with "Level" and "SMO". At the bottom, there are fields for "*Level:" (set to "Level 2") and "*SMO:" (empty), a "Select SMO" button, and "Add/Update Level" and "Remove Level" buttons. A sidebar on the left contains links: "Select Person", "Maintain Security", "Home", "Change Password", "Change Category", "Tutorial", and "Logout".

Figure 12b: Add/Modify/Remove JCAVS User screen (bottom)

Adding a JCAVS User's Account

To add a user's account:

1. From the **Category** drop-down list, select the desired category. When a category is selected from the **Category** drop-down list, the **Grade** field automatically populates.
2. Click on the drop down arrow next to the **Level** box and select the appropriate level(s). Users may be assigned to more than one level.
3. Click on the **Select SMO** button to select the Security Management Office for this user level. The Security Management Office Search screen appears (Figure 9).
4. Type in the SMO Code into the **Code** text box and click **Search**. The screen refreshes and the results of the search are displayed in the lower portion of the screen.
5. Click on the link for the appropriate SMO. The Add/Modify/Remove JCAVS User screen (Figure 12a) returns with the selected SMO displayed in the **SMO** field.
6. Click on the **Add/Update Level** button to add the level. The selection is made and the screen is refreshed.
7. If required, select the **Account Manager** check box (Figure 4). **Note:** Levels 7 and 8 users cannot be account managers.
8. If required, select a **special privilege** under the **Identify Special Privileges** section or **None**, if none is required.

9. If required, select permission under the **Identify Investigation Request Permissions** section (e-QIP).
10. Select the **Add** radio button and click **Save**. The screen refreshes with the new User ID and password. The User ID is located on the Add/Modify/Remove JCAVS User screen. The password is located in the message box.
11. The user's eligibility and investigation are validated when you click the **Save** button. If a user does not meet the requirements for their assigned user level, the system generates an error message. The record is not saved until the user level is corrected or meets the required eligibility and investigation.

Modifying a JCAVS User's Account

An account manager can modify the record of a JPAS user. To modify a user's account:

1. On the Main Menu, click **Select Person**. The Select Person screen appears (Figure 7).
2. Type the **SSN** of the JCAVS user whose account is to be modified and click **Display**. The Add/Modify/Remove JCAVS User screen appears (Figures 12a and b).
3. From the **Category** drop-down list, select the appropriate category to modify.
4. From the **Level** drop-down list, select the appropriate level to modify.
5. Modify the appropriate fields.
6. Scroll to the bottom of the screen, select the **Modify** radio button and click **Save**.

Removing a JCAVS User's Account

A JPAS user whose account has been removed no longer has access to JPAS or any of its components. To remove a user account:

1. On the Main Menu, click **Select Person**. The Select Person screen appears (Figure 7).
2. Type the **SSN** of the JCAVS user whose account you wish to remove and click **Display**. The Add/Modify/Remove JCAVS User screen appears (Figures 12a and b).
3. From the **Category** drop-down list, select the appropriate category to be removed.
4. Scroll to the bottom of the screen, select the **Remove** radio button and click **Save**.

Passwords

When a user is added to the JPAS system, a temporary password is generated. This password must be changed when the user logs in for the first time because system-generated passwords can only be used once. Users are also required to change their password every 60 days - or more often, if he or she deems it necessary, by selecting the **Change Password** option from the JPAS Main Menu. A system-generated message prompting the user to change his or her password will be sent to the user 10 days prior to expiration.

Password Composition

The list below defines password composition.

- Passwords are case-sensitive.
- Passwords must be between 10 and 20 characters in length.
- Passwords must contain at least two different lowercase letters, two different uppercase letters, two different numbers, and two different special characters.
- The new password can not be the same as any of the previous 10 passwords.
- The new password can not be any password used in the previous 18 months.

Changing a Password

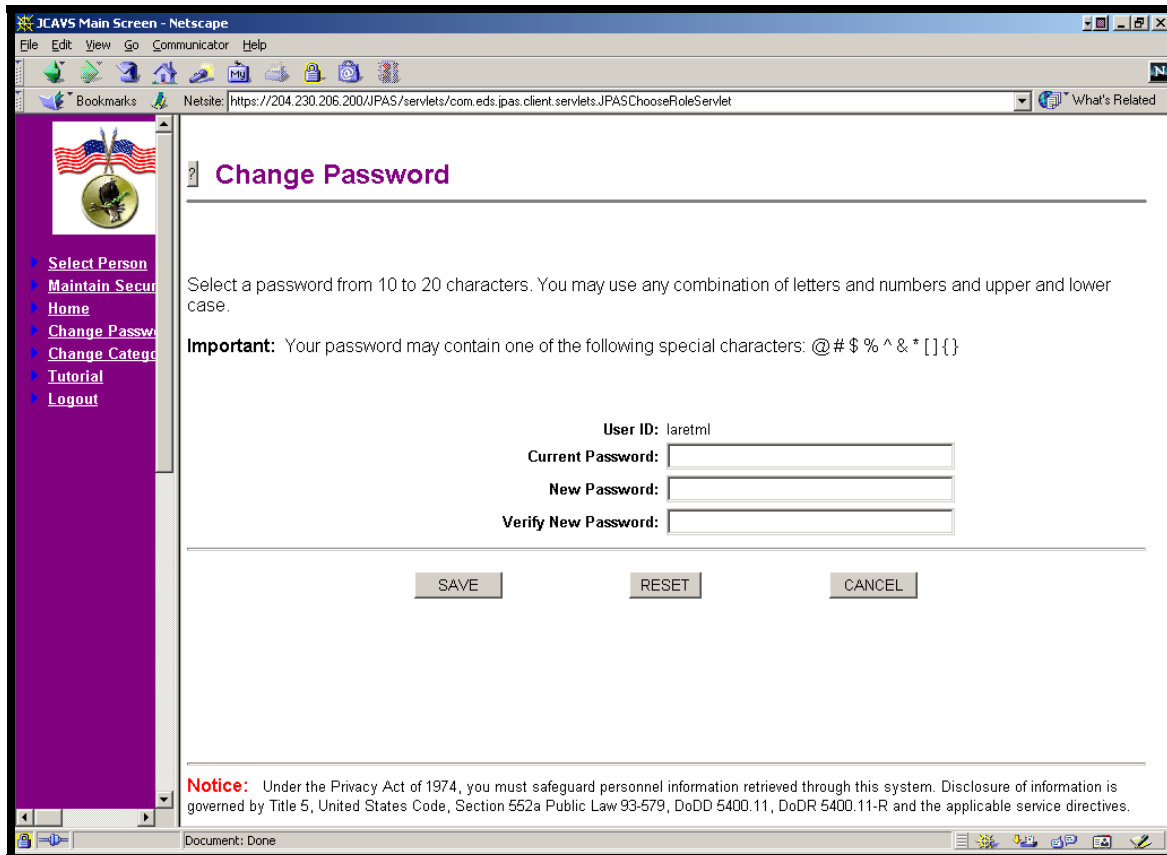
The Change Password screen allows the user to change his or her password at any time once they have successfully logged into the system. To change your password:

1. On the Main Menu, click **Change Password**. The Change Password screen appears (Figure 13).
2. Type your **Current Password**.
3. Type a **New Password**.
4. Retype your new password in the **Verify New Password** text box and click **Save**.

Forgotten Password

If you forget your password, contact your account manager.

Figure 13: Change Password screen



JCAVS Main Screen - Netscape

File Edit View Go Communicator Help

Bookmarks Netsite: https://204.230.206.200/JPAS/servlets/com.eds.jpas.client.servlets.JPASChooseRoleServlet

Change Password

Select a password from 10 to 20 characters. You may use any combination of letters and numbers and upper and lower case.

Important: Your password may contain one of the following special characters: @ # \$ % ^ & * [] { }

User ID: laretml

Current Password:

New Password:

Verify New Password:

SAVE RESET CANCEL

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

Document: Done

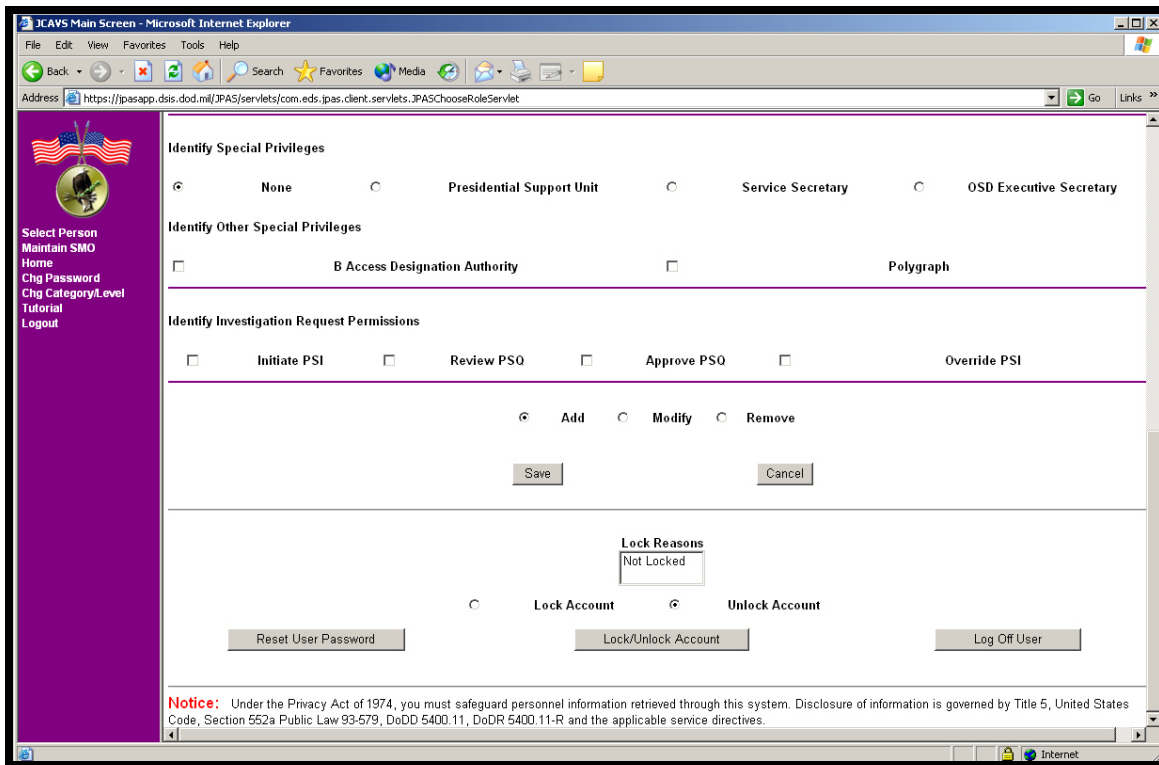
Resetting a User's Password

If a user forgets his or her password, he or she can notify the account manager to have a new password generated using the Reset User Password procedure. If a user feels his or her password has been compromised, the *user* can change the password.

To reset a user's password:

1. On the Main Menu, click **Select Person**. The Select Person screen appears (Figure 7).
2. Type the **SSN** of the JCAVS user whose password is to be reset and click **Display**. The Add/Modify/Remove JCAVS User screen appears (Figures 12a and b).
3. From the **Category** drop-down list, select the appropriate category.
4. Scroll to the bottom of the screen and click the **Reset User Password** button (Figure 14). A new system-generated password is displayed in a dialog box. Record the new password and provide the new password to the user.

**Figure 14: Add/Modify/Remove JCAVS User screen
showing Reset User Password button**



Logging Off a User

The Log Off procedure is performed for users who fail to properly exit the JPAS system from the Main Menu. The next time the user attempts to log in after failing to exit the system properly, they receive a message stating that the User ID is already in use. If this happens, the account manager must log the user out of the system.

To log off a user:

1. On the Main Menu, click **Select Person**. The Select Person screen appears (Figure 7).
2. Type the **SSN** of the JCAVS user who will be logged out of the system.
3. Click **Display**. The Add/Modify/Remove JCAVS User screen appears (Figures 12a and b).
4. From the **Category** drop-down list, select the category of the user to be logged off.
5. Scroll to the bottom of the screen and select the **Log Off User** button (Figure 14). The screen refreshes and the user is logged off.

Locking a User's Account

The account manager has the ability to lock a user's account. If a user's account is locked, the user's access to the system is denied and can only be reinstated by the account manager.

NOTE: The account manager cannot lock or unlock his or her own account.

A user's account is locked after three unsuccessful login attempts or when the account has been inactive for 60 days or more. If a user's eligibility and investigation do not meet the criteria to access the system, the account manager must unlock the account and he or she may be required to modify that account.

To lock a user's account:

1. On the Main Menu, click **Select Person**. The Select Person screen appears (Figure 7).
2. Type the **SSN** of the JCAVS user whose account is to be locked and click **Display**. The Add/Modify/Remove JCAVS User screen appears (Figures 12a and b).
3. From the **Category** on the drop-down list, select the appropriate category.
4. Select the **Lock Account** radio button and click on the **Lock/Unlock Account** button on the Add/Modify/Remove JCAVS User screen (Figure 14). The account is locked.

Unlocking a User's Account

The account manager has the ability to unlock a user's account. If a user's account is locked, access to the system is denied and can only be reinstated by the account manager.

NOTE: The account manager cannot unlock his or her own account.

If a user's eligibility and investigation do not meet the criteria to access the system, the account manager must unlock the account and he or she may be required to modify that account.

To unlock a user's account:

1. On the Main Menu, click **Select Person**. The Select Person screen appears (Figure 7).
2. Type the **SSN** of the JCAVS user whose account is to be unlocked and click **Display**. The Add/Modify/Remove JCAVS User screen appears (Figures 12a and b).
3. From the **Category** drop-down list, select the appropriate category. The field is populated as the selection is made.
4. Select the **Unlock Account** radio button and click on the **Lock/Unlock Account** button on the Add/Modify/Remove JCAVS User screen (Figure 14). The account is unlocked.

Section 4 – How to Establish a Personnel Security Management Network (PSM Net)

Introduction

Establishing and validating your PSM Net is probably the most important and time-consuming part of JCAVS. Your PSM Net is basically a validation list.

Before you initially begin establishing your PSM Net, it is highly recommended that you start with an accurate listing of all cleared personnel. It is also recommended that this list be in alphabetical order.

Instructions

1. Log in as a **User for the SMO in which you want to establish your PSM Net.**
2. Click on **PSM Net** (column on left) to display JCAVS Maintain PSM Net screen (figure 15).

Figure 15: JCAVS Maintain PSM Net screen

NOTE: The first time you access your PSM Net, it will more than likely be empty and not contain any names listed under the **Person Categories**. Once you start “adding” personnel to your PSM Net, they will be listed in alphabetical order under **Person Categories**.

3. Before you begin, check to make sure that the correct SMO and level are indicated in the top left corner under **JCAVS Maintain PSM Net**.
 - a. If not, click on the gray **Select SMO** button.
 - b. Under the **SMO Code** column, click on the correct SMO from the list provided.

NOTE: The SMO will be blue if it has not been clicked during this session or it will be maroon if it has been clicked earlier during this session.

- c. Once you click on the correct SMO, it should take you back to the JCAVS Maintain PSM Net screen (Figure 15).
4. Again, make sure that you have the correct SMO/Level indicated at the top.
NOTE: It is **vital** that you have the correct SMO/Level listed before you proceed!
5. Determine Relationship - owning or servicing. (See definitions.)
6. Now to search the JPAS database, click on the **Person Categories by Organization** radio button.
7. Click the gray **Add** button.
8. You should now be on the PSM Net Add Organization Person Categories screen (Figure 17a).
9. Click on the gray **Select** button.
10. You should now be on the Organization Search screen (Figure 16a).
11. Within the **Search** section, there is a drop down menu right next to **Organization's Service/Agency**. Click on the drop down menu and scroll down until you see your appropriate Service/Agency.
12. In the **Organization UIC/RUC/PASCODE/CAGE** box, type in the Code (All Industry Cage codes will be followed by “-I”) for which you are establishing the PSM Net. **An asterisk (*) can be used for wild card searches when using 3 or more characters.**

Figure 16a: Organization Search screen

The screenshot shows a Netscape browser window titled "JCAVS Main Screen - Netscape". The address bar displays the URL: <https://jpasapp2.osd.mil/JPAS/servlets/com.eds.jpas.client.servlets.JPASChooseRoleServlet>. The browser's menu bar includes File, Edit, View, Go, Communicator, and Help. The toolbar contains icons for Back, Forward, Reload, Home, Search, Guide, Print, Security, and Stop. The bookmarks bar shows "Inside Boeing", "My Information", and "Internet Search".

The main content area is titled "Organization Search". It features a "Selected Organization:" dropdown menu with a "REMOVE" button below it. The "Search:" section includes a dropdown for "*Organization's Service/Agency:" set to "DoD Contractor Companies". Below this is a prompt: "*Enter Search Criteria (include an * for wildcarding):". There are three input fields: "Organization Name:", "Organization Location:", and "Organization UIC/RUC/PASCODE/CAGE:". The "Organization UIC/RUC/PASCODE/CAGE:" field contains the text "0E6K07" and is circled in red. A "SEARCH" button is located below the input fields.

Below the search section is the "Select Organization Search Results:" section, which contains "OK" and "CANCEL" buttons. At the bottom, a "Notice:" states: "Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives."

The left sidebar contains a vertical menu with the following items: "Select Person", "View SMO", "Create/Modify Visit", "Notifications", "Reports", "Access Number", "PSM Net", "Home", "Chg Password", "Chg Category/Level", "Tutorial", and "Logout". The bottom status bar shows "Document: Done" and a taskbar with various application icons, including "Start", "Inbo...", "ASIS...", "JPAS...", "JCAV...", "Docu...", and "Main ...". The system clock in the bottom right corner shows "12:26 PM".

13. Click the gray **Search** button.

14. Under the **Select Organization Search Results** section, you should see the organization code for which you are establishing the PSM Net (figure 16b).

Figure 16b: Organization Search screen (populated)

Organization Search

Selected Organization:

REMOVE

Search:

*Organization's Service/Agency:

*Enter Search Criteria (include an * for wildcarding):

Organization Name:

Organization Location:

Organization UIC/RUC/PASCODE/CAGE:

SEARCH

Select Organization Search Results:

Records 1 - 1 of 1, Page 1 of 1

UIC/RUC/PASCODE/CAGE	Name	Location
0EK07-I	MCDONNELL DOUGLAS CORPORATION	Seabrook

OK CANCEL

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is

15. From the **Select Organization Search Results** on the organization search screen, click on your **organization code**. The organization code will populate in the Selected Organization field.
16. Click on the gray **OK** button.
17. This will take you back to the PSM Net Add Organization Person Categories screen (Figure 17a). The organization code which you selected, should now be listed after **Organization**.

Figure 17a: PSM Net Add Organization Person Categories screen

ICAWS Main Screen - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Guide Print Security Stop

Bookmarks Netsite: https://jpasapp2.osd.mil/JPAS/servlets/com.eds.jpas.client.servlets.JPASChooseRoleServlet

Inside Boeing My Information Internet Search

PSM Net Add Organization Person Categories

SMO: 1D0203 - 1D020 - THE BOEING COMPANY, Level 3

*Relationship: ☒ Owning ☐ Servicing

*Organization: 1D0203 - THE BOEING COMPANY

Eligibility:

Occupation Code:

Access Type:

Search Result for:

SSN	Name	Category	Add
-----	------	----------	-----

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

Document: Done

Start I... R... h... J... J... J... M... U... 6:47 PM

18. Click the gray **Search** button.
 19. Under the **Search Result for** section, you will see everyone that, according to the JPAS database, belongs to the organization code you selected. (Figure 17b)
 20. Using your list of cleared personnel, you have two options to add personnel to your PSM Net.
 - a. Option 1- Click on the **Add All** button at the bottom of the screen. This adds all categories associated to that personnel record.
 - b. Option 2- Check the **Add** box at the far right after each name. Once you have completed a page, click on the **Add** button at the bottom of the page.
- NOTE:** Make sure you click the **Add** button at the bottom of each page BEFORE you move to the next page – if you do not, the names are unchecked by the system.

After you click the **Add** button at the bottom of the page, the same page will “refresh” and add

the equivalent number of new names at the bottom of the page that you added to your PSM Net. For example, if you are on the first page and you “add” ten people from that page to your PSM Net, when the page refreshes itself, there will be ten “new” names listed at the bottom of the page that came from the top of the second page. If you add three of those names to you PSM Net, when the page refreshes, there will be three new names at the bottom of the page.

Once you have added everyone you want from the first page, continue on with the remaining page(s) until you have added everyone within your PSM Net.

Figure 17b: PSM Net Add Organization Person Categories screen (results)

PSM Net Add Organization Person Categories

SMO: S10207 - UC15 Add/Modify/Cancel A Visit S10207, Level 2

***Relationship:**
☒ Owning
 ☐ Servicing

***Organization:** WDFKA1 - 0002 MI CTR ELE PENTAGON

Select Organization

Eligibility:

Occupation Code:

Access Type:

Search

Search Result for: WDFKA1 - 0002 MI CTR ELE PENTAGON, Owning

Records 1 - 3 of 4, Page 1 of 2

1

2

Next

Last

Sort/Find By:

Last Name

☒ Ascending
 ☐ Descending

Sort

Find:

Find

SSN	Name	Category	Add
000-00-1234	ALLEN, GEORGE KITCHENER	Active Duty	<input type="checkbox"/>
000-00-5678	HARRIS, SCOTT STIRLING	Active Duty	<input type="checkbox"/>
000-00-9012	MURRAY, MICHELLE MARIE	Active Duty	<input type="checkbox"/>

Add

Add All

Cancel

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

21. If you did not find everyone on your list during this process, most likely it is because the missing personnel are not assigned a category containing your organization. You can also populate your PSM-Net according to SSN by following the same steps above until you reach step 8. Once in the JCAVS Maintain PSM Net screen (Figure 15), select **Person Categories by SSN** and select the correct category. If no record exists in system wait for data field or refer to Section 5, “How to add a Record – (Industry Only).”

Section 5 – How to Add a Record (Industry Only)

Introduction

*If you attempt to “lookup” a person’s record in JCAVS and receive an error message that the person does not exist, then there is no record within JPAS for that person. **First make sure you entered the correct SSN.** If you are sure you entered the correct SSN and still received the error message that the person does not exist, you will have to create a record within JPAS for this person. (Non DOD Categories only)*

Examples: A person is being submitted for his/her initial investigation and eligibility:

For Industry personnel, if you have a person(SSN), and there is no record in JPAS, you will have to establish a JPAS record. Then you will have to “in-process” (Section 7) this record into your PSM Net so you can submit a Request to Research Upgrade Eligibility (RRU) (Section 11) to the Defense Industrial Security Clearance Office (DISCO) to inform them of the existing status .

Instructions

1. Log in as a **User**.
2. Click on **Select Person** (column on left).
3. Enter the person’s **SSN**.
4. Click the **Display Add/Modify Non-DoD Person** radio button.
5. Click the gray **Display** button.
6. The **Add/Modify Non-DoD Person** screen (Figure 18) will appear.
7. Enter all the information on the person in the blank fields.

Figure 18: Add/Modify Non-DoD Person screen

JCAVS Main Screen - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <https://jpasapp2.osd.mil/JPAS/servlets/com.eds.jpas.client.servlets.JPASChooseRoleServlet> Go Links

Add/Modify Non-DoD Person

SSN: 234-56-7891

*Last Name: *First Name: Middle Name: Cadency:

*DOB: *Citizenship: Date of Death:

State of Birth: *Country of Birth:

Eligibility: N/A
Investigation: N/A
Open Investigation: N/A
Incident Report: N/A
Polygraph: N/A

Foreign Relation:

Available Category Types:

Person Category: Position:

Category Classification: (Required for Industry Categories)

Select Person
View SMO
Create/Modify Visit
Notifications
Reports
PSM Net
Home
Chg Password
Chg Category/Level
Tutorial
Logout

Done Internet

Start In... ht... e... JP... JP... JC...

2:40 PM

8. Create a **Category** for the person. (Refer to Section 6 – **How to Add a Category**).
9. Click the gray **Save** button to save personal identifying data (PID) information.

NOTE: If you are planning to submit the person for their initial investigation via e-Qip, all information in sections 5, 6, 7 and 10 must be completed. If the person already has a current eligibility, “in-process” the person (Refer to Section 7 – “How to In-Process”) and submit an RRU (Refer to Section 14 – “How to Generate a Request to Research/Upgrade Eligibility”) to the appropriate Central Adjudication Facility (CAF).

Section 6 – How to Add a Category (Industry Only)

Introduction

If you want to add a record to your PSM Net, the first thing you need to ensure is that the record has the correct “category” that you want to add to your PSM Net. If the record does not have the correct “category,” then you will need to add a new category to the person’s record. (Industry Only)

Instructions

1. Log in as a **User**.
2. Click **Select Person** (column on left).
3. Enter the person’s **SSN**.
4. Click the **Display Add/Modify Non-DoD Person** radio button.
5. Click the gray **Display** button.
6. In the **Available Category Types** drop down, make sure you choose the proper category. Examples: Red Cross, Seasonal Employees, Industry, etc.
7. Click **Add Category** button.
8. In the **Category Classification** drop down box, select one of the five options. In most cases you will select **Contractor** with the exception of an FSO where you will select **Key Management Personnel (KMP)**. Other employees that are listed on your organization’s KMP list must also be listed as a KMP in JPAS. Other new choices are Assurance 1 and Assurance 2.
9. In the **Service Agency** drop down box, select the correct service. For Industry it is very important to select **DoD Contractor Companies**.
10. Click on the gray **Modify Organization** box.
11. In the **Organization's Service/Agency** drop down box, scroll down until you reach the appropriate organization.
12. In the **Organization UIC/RUC/PASCODE/CODE** text box, type in the organization code. **An asterisk (*) can be used for wild card searches when using 3 or more characters.**

Figure 19a: Organization Search screen

The screenshot shows a Netscape browser window titled "JCAVS Main Screen - Netscape". The address bar displays the URL: `https://jpasapp2.osd.mil/JPAS/servlets/com.eds.jpas.client.servlets.JPASChooseRoleServlet`. The browser's menu bar includes File, Edit, View, Go, Communicator, and Help. The toolbar contains icons for Back, Forward, Reload, Home, Search, Guide, Print, Security, and Stop. Below the toolbar, there are links for Bookmarks, Netsite, Inside Boeing, My Information, and Internet Search.

The main content area is titled "Organization Search". It features a "Selected Organization:" dropdown menu with a "REMOVE" button below it. The "Search:" section includes a dropdown for "*Organization's Service/Agency:" set to "DoD Contractor Companies". Below this is a prompt: "*Enter Search Criteria (include an * for wildcarding):". There are three input fields: "Organization Name:", "Organization Location:", and "Organization UIC/RUC/PASCODE/CAGE:". The "Organization UIC/RUC/PASCODE/CAGE:" field contains the text "0EK07*", which is circled in red. A "SEARCH" button is located below these fields.

Below the search fields is a section titled "Select Organization Search Results:" with "OK" and "CANCEL" buttons. At the bottom, a "Notice:" states: "Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives."

The left sidebar contains a vertical menu with the following items: Select Person, View SMO, Create/Modify Visit, Notifications, Reports, Access Number, PSM Net, Home, Chg Password, Chg Category/Level, Tutorial, and Logout. The bottom of the browser window shows a taskbar with various application icons and a system clock displaying 12:26 PM.

13. Click the gray **Search** button.

14. Under **Select Organization Search Results** section, you should see the Organization code based on your search.

Figure 19b: Organization Search screen (results)

JCAVS Main Screen - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Guide Print Security Stop

Bookmarks Netsite: https://ipasapp2.osd.mil/JPAS/servlets/com.eds.ipas.client.servlets.JPASChooseRoleServlet

Inside Boeing My Information Internet Search

Organization Search

Selected Organization:

REMOVE

Search:

*Organization's Service/Agency: DoD Contractor Companies

*Enter Search Criteria (include an * for wildcarding):

Organization Name:

Organization Location:

Organization UIC/RUC/PASCODE/CAGE: 0EK07*

SEARCH

Select Organization Search Results:

Records 1 - 1 of 1, Page 1 of 1

UIC/RUC/PASCODE/CAGE	Name	Location
0EK07-I	MCDONNELL DOUGLAS CORPORATION	Seabrook

OK CANCEL

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is

Document: Done

Start Inbo... ASIS... JPAS... JCAV... Docu... Main ... 12:37 PM

15. Under the **UIC/RUC/PASCODE/CAGE** section, click on the appropriate **organization code** hyperlink. This will populate the **Selected Organization** field.
16. Click on the gray **OK** button.
17. The organization code you selected should now be listed in the **Organization/Company/Agency** section on the Add/Modify non DoD Person screen (Figure 20).

Figure 20: Add/Modify Non- DoD Person screen (bottom)

JCAVS Main Screen - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Guide Print Security Stop

Bookmarks Netsite: https://jpasapp2.osd.mil/JPAS/servlets/com.eds.jpas.client.servlets.JPASChooseRoleServlet

Inside Boeing My Information Internet Search

Incident Report: N/A
Polygraph: N/A

Foreign Relation: N/A MODIFY RELATIONSHIP

Available Category Types: Non-DoD National Guard ADD CATEGORY

Person Category: Industry 2 (0) Position:

Category: Contractor
Classification: (Required for Industry Categories only)

Separation Date: Separation Code:

Organization/Company/Agency MODIFY ORGANIZATION

Name: MCDONNELL DOUGLAS CORPORATION
Location: 10210 Greenbelt Road, Seabrook, MD, 207062218

[Person Summary](#)

SAVE CANCEL

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

Document: Done

Start Inbo... ASIS... JPAS... JCAV... Docu... Main ... 12:43 PM

Screen Print 4-3

18. Click on the gray **Save** button.
19. Check to see if the newly established code is displayed in the **Person Category** field.
20. Click on the **Person Summary** hyperlink to ensure the newly established person category is created. You will be on the person summary screen.
21. Once verified, click **Cancel** at the bottom of the person summary. You will go back to the Add/Modify/Non-DoD person screen (Figure 18).
22. If the new category is not there, repeat steps 1-18.

Section 7 – How to In-Process

Introduction

When you in-process a person, you are adding individual categories to the PSM Net of your SMO. There are several instances when you will in-process a person into the PSM Net of your SMO, such as:

- *When adding categories to your established PSM Net.*
- *When an employee transfers from one SMO to another SMO.*
- *When a new hire or current employee requires access.*

The most important thing to remember when in-processing an employee is to make sure you in-process the correct category. If not, and you enter an “In Date” for this person, you will assign the wrong category to your PSM Net.

NOTE: Refer to Section 4 – **How to Establish a PSM Net** if adding groups of categories by organization or adding from PSM Net screen.

Instructions

1. Log in as a **User for the SMO where you are adding the employee.**
2. Click on **Select Person** (column on left).
3. Enter person's SSN.
4. Click the **Person Summary** radio button.
5. Click the gray **Display** button.
6. When the Person Summary screen appears (Figure 8), **make sure the appropriate category is displayed.**
7. Click the **In/Out Process** hyperlink located in the **Person Category Information** section to display the “View/Modify In/Out” screen (Figure 21).
8. Click on the gray **Select SMO** box to ensure the correct SMO is listed.
9. To select the SMO with which you have a parent relationship, enter today's date in the **In Date** box (Format: YYYY MM DD), or click the calendar and choose the date.
10. Next to **Relationship**, click the **Owning** or **Servicing** radio box.
11. **Click** the gray **Save** button.
12. Under the **View/Modify Active Relationship(s)** section, the newly established organization code should be listed under **In Date**.

Figure 21: View/Modify In/Out screen

View/Modify In/Out

HILL, JOHN S

SSN:
Grade: GS
Category: Civilian Employee (DOD)

Owning SCI SMO: N/A
Owning Non-SCI SMO: DSSHQSEC - DEFENSE SECURITY SERVICE, HEADQUARTERS SECURITY, Level 4, 703-325-9458/9638,

Add New Relationship

* SMO: DSSTEST - DEFENSE SECURITY SERVICE, SETA, TEST, Level 3

Select SMO

* In Date:

Out Date:

* Relationship:
☐ Owning
☐ Servicing

View/Modify Active Relationship(s)

Code	Name	Location	Level	In Date	Out Date	Relationship	Change
DSSAPS6	DEFENSE SECURITY SERVICE, DSSA	LINTHICUM, MD	Level 6	2005 05 05	N/A	Servicing	<div>Reason</div>
DSSHQSEC	DEFENSE SECURITY SERVICE, HEADQUARTERS SECURITY	ALEXANDRIA, VA	Level 4	2003 01 10	N/A	Owning	<div>Reason</div>
DSSTEST	DEFENSE SECURITY SERVICE, SETA, TEST	LINTHICUM, MD	Level 3	2005 07 13	<div></div> <div></div>	Servicing	<input type="checkbox"/>

Save

Cancel

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

Section 8 – How to Indoctrinate

Introduction

The term “indoctrinate” within JPAS means you are going to assign an “access” level to a cleared employee. For example, if you want to give a person who currently possesses a final SSBI, access to Top Secret information, you will need to “indoctrinate” that person at the Top Secret access level. Once a person is indoctrinated at an access level, they will remain at that level until you debrief them.

Each person within your PSM Net can be indoctrinated at an access level once they have eligibility, or an interim approval.

NOTE: Just because a person has a current final SSBI, does not mean you have to indoctrinate them at the Top Secret level. It all depends on the level of information they are going to be accessing in the performance of their job. You can always change their access level, if required.

Instructions - Non-SCI Indoctrination

1. Log in as a **User for the SMO** where you are indoctrinating the employee.
2. Click on **Select Person** (column on left).
3. Enter the person’s **SSN**.
4. Click on the **Person Summary** radio button.
5. Click on the gray **Display** button.
6. Make sure the category box located within the **Personal Identification** section is displaying the correct SMO. If the correct SMO is not being displayed, click on the drop down box and scroll down and highlight the correct SMO.

NOTE: When the “Person Summary” screen first appears and you get an error message that says *The Person Category does not have any Owning/Servicing Relationship and no Notification based on Owning/Servicing Relationship will be sent*, then the listed category is not currently in a PSM Net.

7. Scroll down to the **Accesses** section. This section displays access information in columns according to Person Category (Figure 22). If no information exists for any Person Category, the column does not display. Under this section you will normally see 4 columns: **Category**, **PSP**, **Suitability and Trustworthiness** and **SCI**. If you have a PSM Net relationship and the member meets requirements for indoctrination, you will see an **Available Action** column. If you see Top Secret, Interim Top Secret, Secret, Interim Secret or Confidential listed under **US Access**, then that person has already been indoctrinated at that level. If there is nothing listed under the **US Access** column, then that person has not been indoctrinated at any level and you will be required to indoctrinate that person.

NOTE: If no access information exists for any Person Category, the column does not display. If the **Indoctrinate** hyperlink does not appear, then most likely the person you are trying to indoctrinate does not meet eligibility and investigation requirements or has not been in-processed into the PSM-Net of your SMO. To add a person to your PSM-Net, refer to Section 7 – **How to In-Process**. Once you have added the person to your PSM-Net, the available actions column will appear.

8. Click on the **Indoctrinate** hyperlink to indoctrinate a person.

Figure 22: Person Summary (accesses) screen

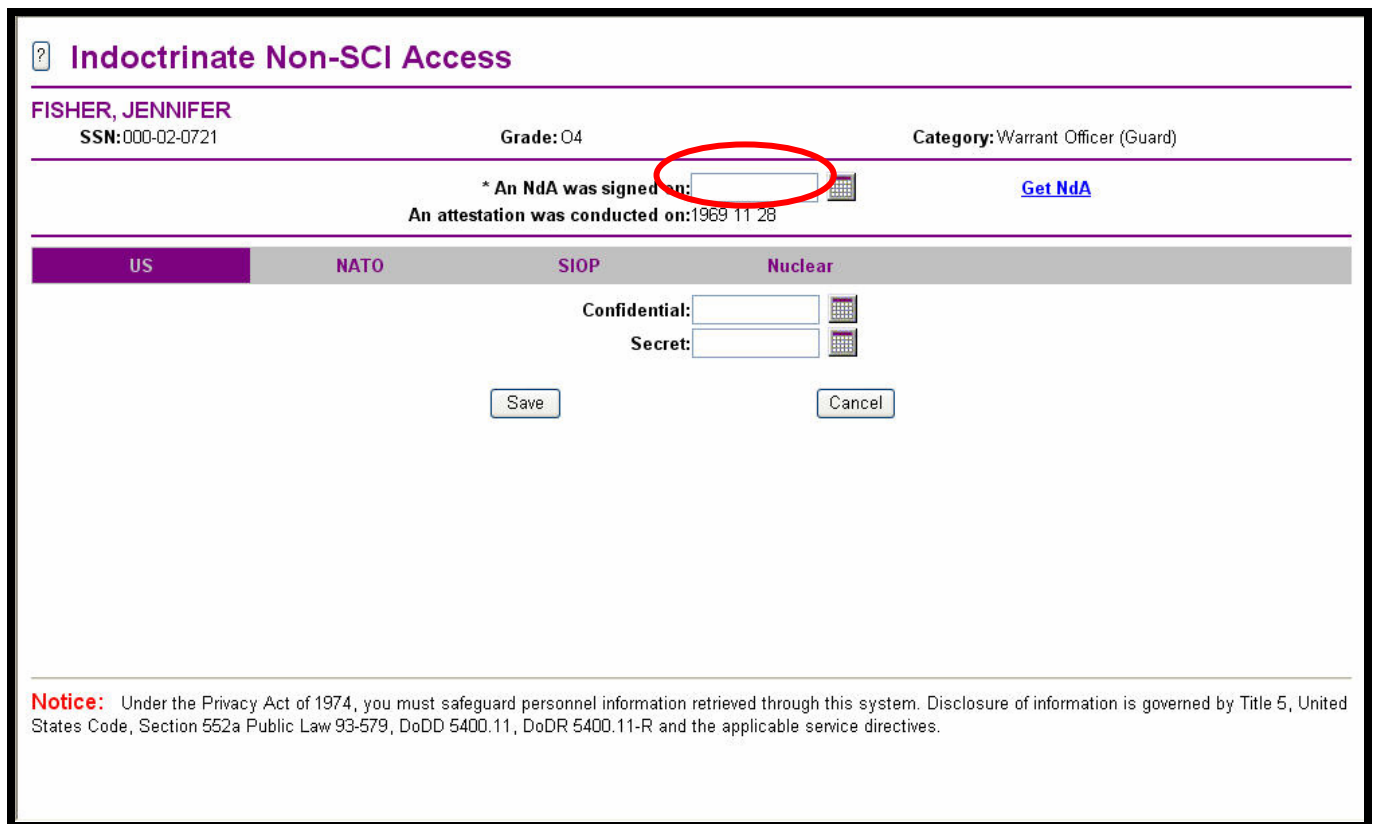
Accesses									
Category	US Access	NATO Access	Nuclear	PSP	SIOP	Suitability and Trustworthiness	SPA	SCI	Available Actions
Active Duty - Enlisted (USN)				No		IT: N/A Public Trust: N/A Child Care: N/A	2004 02 13 - 2005 01 06	Access Number: N/A	Indoctrinate Non-SCI Debrief Non-SCI Indoctrinate SCI Debrief SCI

- In the Personal Identification section of the Person Summary screen (Figure 23a), you will see: ***An NdA was signed: YES, NO or N/A.**

If there is a date or yes populating the entry field, then the person has already signed a Non-Disclosure Agreement (NdA) and the NdA is already on file with the appropriate agency. However, if the entry field is blank, NO, or N/A, you will need to have the person sign a non-disclosure agreement and enter the date that they signed.


NOTE: There **must** be a date in the NdA block before JPAS will allow you to grant a person any level of access.

Figure 23a: Indoctrinate Non-SCI Access screen





Indoctrinate Non-SCI Access

FISHER, JENNIFER
SSN: 000-02-0721 Grade: O4 Category: Warrant Officer (Guard)

* An NdA was signed on:  [Get NdA](#)
An attestation was conducted on: 1969 11 28

US NATO SIOP Nuclear

Confidential: 
Secret: 

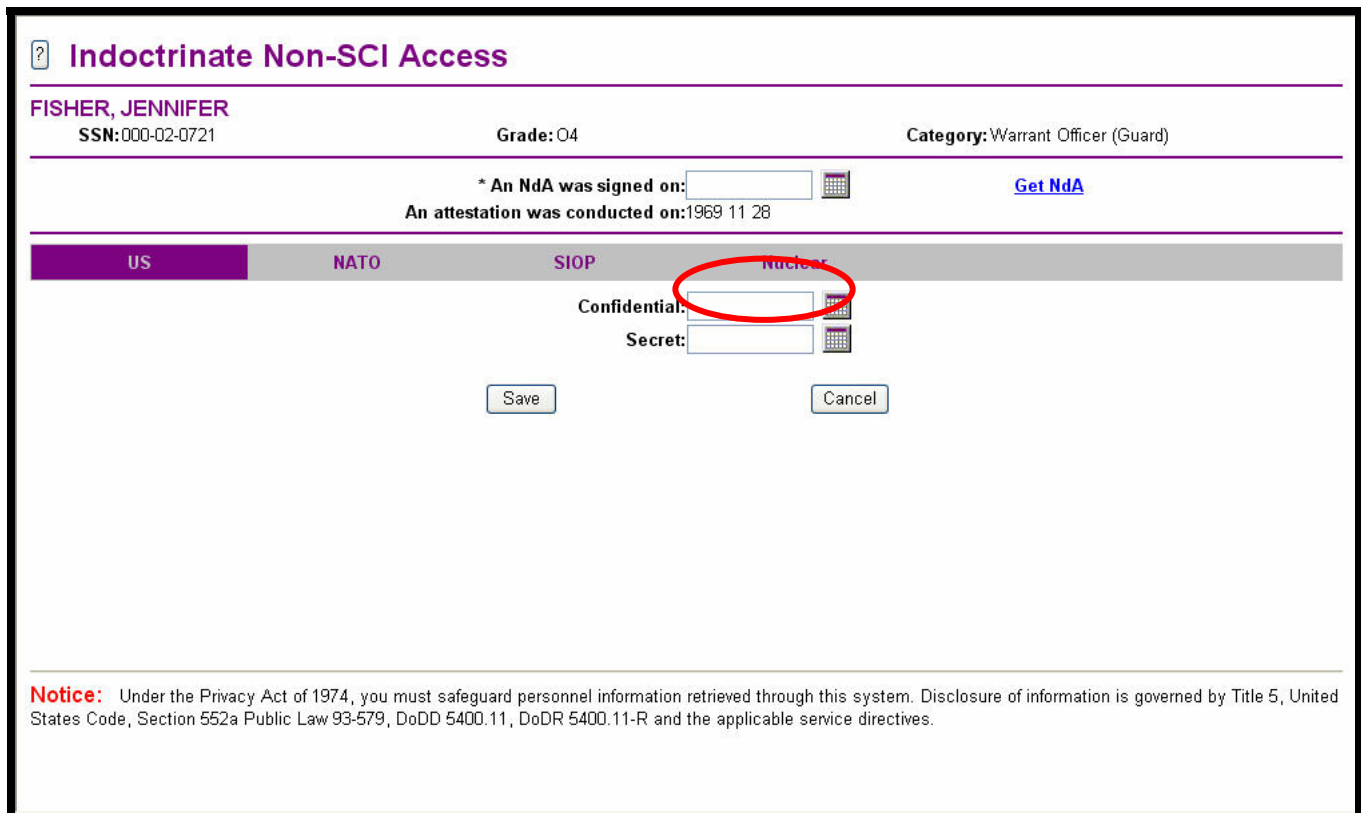
Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

10. Below the NdA data field, you will see four (4) tabs identified as **US**, **NATO**, **SIOP** and **Nuclear**. If you click on any one of these tabs, the entry fields for that particular tab will appear. For example, when you click on the **US** tab, you will be provided with the entry fields that are appropriate for that tab based on that person's eligibility. In another example, if the person has a final SSBI investigation, you will see entry fields labeled **Attestation**, **Confidential**, **Secret** and **Top Secret**. However, if the employee only has a final NACLC, you will NOT see an entry field for **Top Secret**.
11. If a person has been briefed for Restricted Data (RD) or Critical Nuclear Weapon Design Information (CNWDI) click on the **Nuclear** tab and enter the date briefed.

Another reminder: Just because an employee has a current SSBI investigation, does not mean you have to indoctrinate them for Top Secret access. You should indoctrinate them commensurate with the classification level of information required by them to do their job.


Once you have decided on what "access" level you want to indoctrinate a person, enter the date you are granting the access.

Figure 23b: Indoctrinate Non-SCI Access screen




Indoctrinate Non-SCI Access


FISHER, JENNIFER
SSN: 000-02-0721
Grade: O4
Category: Warrant Officer (Guard)

* An NdA was signed on:  [Get NdA](#)

An attestation was conducted on: 1969 11 28

US NATO SIOP **Nuclear**

Confidential: 

Secret: 

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

12. Once you have entered the date, click on the **Save** button.
13. The “entry field” where you entered the date should go away (become solid). Once you click the **Save** button, the only way you can change this date is to “debrief” this person from that access level. (Refer to Section 9 – **How to Debrief**)
14. Click on the gray **Cancel** button and this will take you back to the Person Summary screen (Figure 24a). If you scroll down to the **Accesses** section, you will see the access level.

Figure 24a: Person Summary screen

Coast Guard (USCG)	Top Secret (Cosmic TS)	Atomic S		Yes		IT: N/A Public Trust: N/A Child Care: No		SI Access Number: N/A	Indoctrinate Non-SCI Debrief Non-SCI Grant Interim Indoctrinate SCI Debrief SCI Request SPA
Industry (Contractor) 1259U	Interim Secret	NATO C NATO S Cosmic TS Atomic C Atomic S Atomic TS	CNWDI PRP Crit Rest Data SIGMA 16	No	SIOP2 SIOP3 SIOP4 SIOP5	IT: 2 Public Trust: Yes Child Care: Yes		SI, TK, C4, B Access Number: 00000345671	Debrief Non-SCI Debrief SCI

15. You can use this same process for indoctrinating personnel who have been briefed for NATO, CNWDI, SIGMA 16, SIOP or Restricted Data.

Instructions - SCI Indoctrination

1. Log in as a **User for the organization where you are indoctrinating the employee.** (SCI Indoctrination requires the User to be logged in as a Level 2 or Level 3).
2. Click on **Select Person** (column on left).
3. Enter the person's **SSN**.
4. Click on the **Person Summary** radio button.
5. Click on the gray **Display** button.
6. Make sure the category box located within the **Person Category** section is displaying the correct category. If the correct category is not being displayed, click on the drop down box and scroll down and highlight the correct category.

NOTE: When the Person Summary screen first appears and you get an error message that says, *The Person Category does not have any Owning/Servicing Relationship and no Notification based on Owning/Servicing Relationship will be sent*, then the listed category is not currently in a PSM Net.
7. Scroll down to the **Accesses** section (Figure 24b). Under the **SCI** column you will see "Access Number" listed. If you are logged in as a Level 2, 3 or 8 User, and the person has been indoctrinated into an SCI compartmented program, then you will see the compartmented acronyms listed next to "Access." If you are logged in at any other User level, then you will only see "Yes" listed next to "Access." If there is an "N/A" or a "No" listed next to "Access," then that person has not been indoctrinated into any SCI compartmented programs and you will be required to indoctrinate that person.

Figure 24b: Person Summary screen

Accesses

Category	US Access	NATO Access	Nuclear	PSP	SIOP	Suitability and Trustworthiness	SPA	SCI	Available Actions
Active Duty - Enlisted (USN)				No		IT: N/A Public Trust: N/A Child Care: N/A	2004 02 13 - 2005 01 06	Access Number: N/A	Indoctrinate Non-SCI Debrief Non-SCI Indoctrinate SCI Debrief SCI
Coast Guard (USCG)	Top Secret	Cosmic TS Atomal S		Yes		IT: N/A Public Trust: N/A Child Care: No		SI Access Number: N/A	Indoctrinate Non-SCI Debrief Non-SCI Grant Interim Indoctrinate SCI Debrief SCI Request SPA
Industry (Contractor) 1259U	Interim Secret	NATO C NATO S Cosmic TS Atomal C Atomal S Atomal TS	CNWDI PRP Crit Rest Data SIGMA 16	No	SIOP2 SIOP3 SIOP4 SIOP5	IT: 2 Public Trust: Yes Child Care: Yes		SI, TK, C4, B Access Number: 00000345671	Debrief Non-SCI Debrief SCI

Indoctrination Link

No Indoctrinations

- To indoctrinate a person, click on the **Indoctrinate** hyperlink.

NOTE: If the **Indoctrinate** hyperlink does not appear, the person you are trying to indoctrinate has not been assigned to the PSM-Net of your SMO or does not meet eligibility requirements. To add personnel to your PSM-Net refer to Section 7 – **How to In-Process**. Once you have added the person to your PSM-Net and they meet the eligibility requirements, the **Available Action** hyperlink should appear.

- Once at the Indoctrinate SCI Access screen, before you can indoctrinate a person into any SCI compartmented program, you must first ensure that the person has signed both the “Non-Disclosure Agreement” (NdA) and the “Non-Disclosure Statement” (NdS). Enter the dates (Format: YYYY MM DD) in which the person signed both the NdA and the NdS in the appropriate entry field. (Figure 25a)

*An NdA was signed on:

*An NdS was signed on:

If there is a date already populating the appropriate entry fields, then both the NdA and the NdS have already been registered. If the appropriate entry field is blank, you will need to have the person sign an NdA and NdS before you can continue. NDA/ND S.

Figure 25a: Indoctrinate SCI Access screen

?

Indoctrinate SCI Access

FISHER, JENNIFER

SSN: 000-02-0726

Grade: O4

Category: Warrant Officer (Guard)

* An NdA was signed on: 2000 09 19

[Get NdA](#)

* An NdS was signed on:

[Get NdS](#)

An attestation was conducted on:

SI:

G:

EU:

HSL:

HCS:

TK:

EL:

NK:

C4:

B:

Save

Cancel

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

10. Below the NdA & NdS data field, you will see SCI compartmented program designators listed. Each designator has an entry field immediately to the right.
11. Enter the date in the entry field for the compartments for which the person has been briefed. (Figure 25b)

Figure 25b: Indoctrinate SCI Access screen

?

Indoctrinate SCI Access

FISHER, JENNIFER

SSN: 000-02-0726

Grade: O4

Category: Warrant Officer (Guard)

* An NdA was signed on: 2000 09 19

[Get NdA](#)

* An NdS was signed on:

[Get NdS](#)

An attestation was conducted on:

SI:

G:

EU:

HSL:

HCS:

TK:

EL:

NK:

C4:

B:

Save

Cancel

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

12. Once you have entered the date, click on the **Save** button.
13. The “entry field” where you entered the date should go away (become solid). Once you click the **Save** button, the only way you can change this date is to “debrief” this person and then re-indoctrinate. (Refer to Section 9 – **How to Debrief**)
14. Click on the gray **Cancel** button to return to the Person Summary screen. If you scroll down to **SCI** in the **Accesses** section, you will see immediately to the right of “Access,” the compartmented program designators indicating that the person has been briefed.

Section 9 – How to Debrief

Introduction

The term “debrief” within JPAS means you are going to remove the person’s level of “access.” For example, if a person no longer requires access to Top Secret information and only requires access at the Secret level, you will “debrief” that person from the Top Secret access level and then indoctrinate that person at the Secret level.

Instructions (Debrief-Non-SCI Accesses)

1. Log in as a **User for the SMO where you are debriefing the employee.**
2. Click on **Select Person** (column on left).
3. Enter the person’s **SSN**.
4. Click on the **Person Summary** radio button.
5. Click on the gray **Display** button.
6. Make sure the category box located within the **Person Category** section is displaying the correct organization. If the correct organization is not being displayed, click on the drop down box and scroll down and highlight the correct organization.

NOTE: When the Person Summary screen first appears and you get an error message that says, *The Person Category does not have any Owning/Servicing Relationship and no Notification based on Owning/Servicing Relationship will be sent*, then the listed category is not currently in a PSM Net.

7. Scroll to the **Accesses** section (Figure 26). This section displays Access information that is arranged in columns by **Person Category**. If no information exists for any **Person Category**, the column does not display. If you see Top Secret, Interim Top Secret, Secret, Interim Secret or Confidential listed under **US Access** or accesses under any Non SCI column, then that person has already been indoctrinated at that level and those accesses can be debriefed.
8. To debrief a person, click on the **Debrief Non-SCI** hyperlink. If there were no accesses assigned, this hyperlink will not appear.

Figure 26: Person Summary (Accesses) screen

Person Summary

HARBACK, HELEN K
Person Category

Industry (Contractor) HH3VFDBB

SSN: 926-60-5777

Open Investigation: N/A

PSQ Sent Date: N/A

Attestation Date: N/A

Incident Report: N/A

SF 713 Fin Consent Date: N/A

SF 714 Fin Disclosure Date: N/A

Polygraph: N/A

Foreign Relation:

N/A

[PSQ Sent](#)
[Non-SCI Access History](#)
[Unofficial Foreign Travel](#)
[NdS History](#)

Date of Birth: 1966 05 17

Marital Status: N/A

Place of Birth: New York

Citizenship: U.S. Citizen

NdA Signed: Yes

NdS Signed: Yes

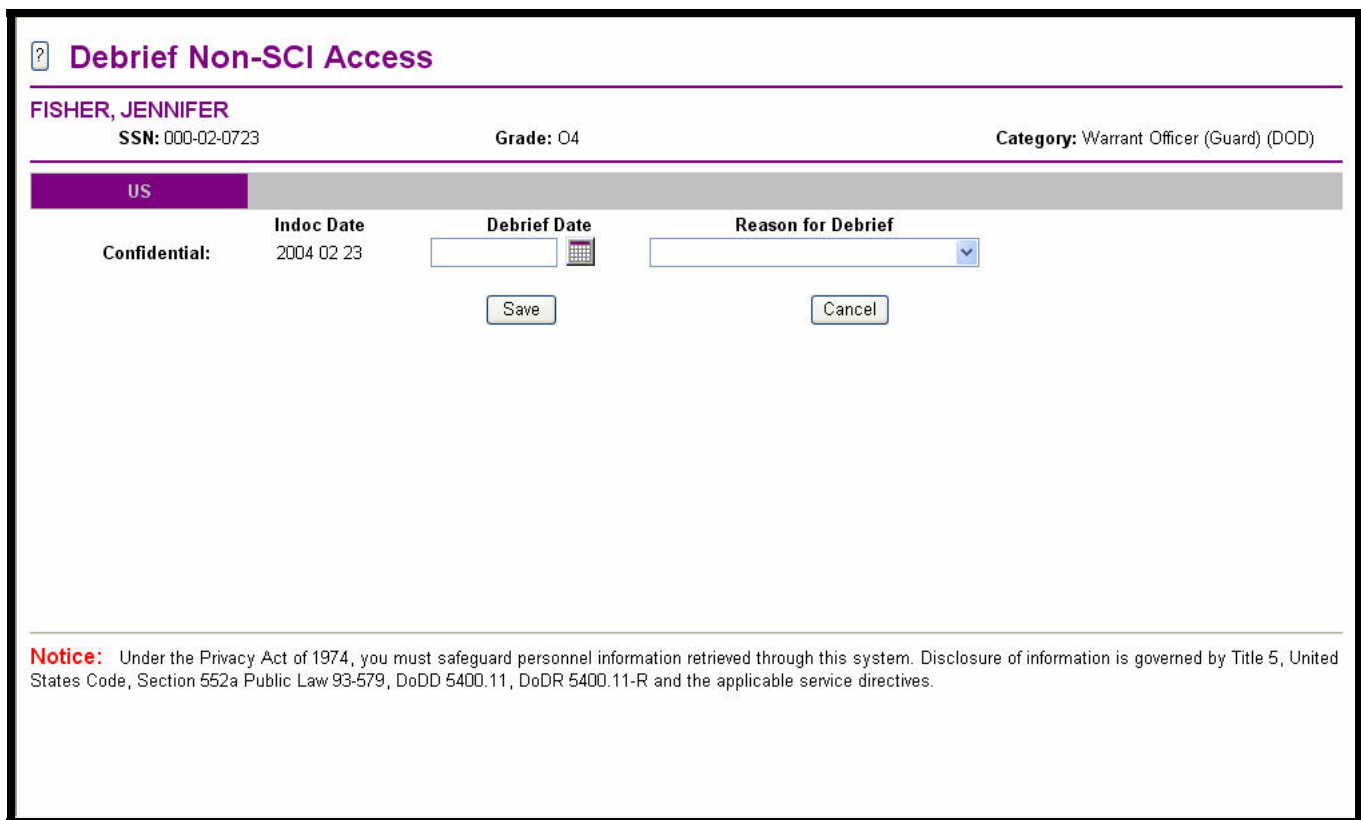
[SCI Access History](#)
[Request to Research/Upgrade Eligibility](#)
[NdA History](#)

Accesses

Category	US Access	PSP	Suitability and Trustworthiness	SCI	Available Actions
Industry (Contractor) HH3VFDBB	Top Secret	No	IT: N/A Public Trust: N/A Child Care: N/A	Access Number: N/A	Indoctrinate Non-SCI Debrief Non-SCI Indoctrinate SCI Request SPA
Industry (Contractor) 7N699-I		No	IT: N/A Public Trust: N/A Child Care: N/A	Access Number: N/A	
Industry (Contractor) 0S482-I	Top Secret	No	IT: N/A	SI	Indoctrinate Non-SCI

- A list will appear containing all the “accesses” for which the person is currently indoctrinated. (Figure 27)



Figure 27: Debrief Non-SCI Access screen



Debrief Non-SCI Access

FISHER, JENNIFER
SSN: 000-02-0723 Grade: O4 Category: Warrant Officer (Guard) (DOD)

US

Confidential: Indoc Date: 2004 02 23 Debrief Date:  Reason for Debrief: 

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

10. Enter a **Debrief Date** and select a **Reason for Debrief** from the drop down box. If you do not select a reason for the debriefing, you will receive a dialog box indicating the system will not perform the debriefing.

NOTE: You will notice that the choices listed in the **Reasons for Debrief** drop down box are generally more applicable for those in the military. For example, there is no reason code for Multiple Facility Transfer (MFT); however the “Permanent Change of Station” could be used as a work around.

11. Click the gray **Save** button and the access is removed.
12. Click on the gray **Cancel** button and it will return you to the person’s Person Summary screen.
13. Make sure you are using the available action column for the correct category showing in the **Accesses** section.
14. There will be no accesses in the appropriate column for the selected category. **Note:** If no information exists for any **Person Category**, the column does not display.

Instructions (Debrief-SCI Accesses)

1. Log in as a **User for the SMO where you are debriefing the employee.**
2. Click on **Select Person** (column on left).
3. Enter the person's **SSN**.
4. Click on the **Person Summary** radio button.
5. Click on the gray **Display** button.
6. Make sure the category box located within the **Person Category** section is displaying the correct organization. If the correct organization is not being displayed, click on the drop down box and scroll down and highlight the correct organization.

NOTE: When the Person Summary screen first appears and you get an error message that says, *The Person Category does not have any Owning/Servicing Relationship and no Notification based on Owning/Servicing Relationship will be sent*, then the listed category is not currently in a PSM Net.

7. Scroll down to **SCI** in the **Accesses** section (Figure 28). Under the SCI column you will see "Access" and "Access Number" listed. (Figure 25a)
 - If you are logged on as a Level 2 or 3 User, you will see the designators listed under the **SCI** column for the compartmented program(s) in which the person is briefed. If the person is not briefed to any compartmented programs, you will see "Access Number: N/A."
 - If you are logged in as a Level 4 User or lower, you will see "Yes" in the **SCI** column. If the person is not briefed to any compartmented programs you will see "Access Number: N/A."
8. To debrief a person, click on the **Debrief** hyperlink.

Figure 28: Person Summary (Accesses) screen

Accesses					
Category	US Access	PSP	Suitability and Trustworthiness	SCI	Available Actions
Industry (Contractor) HH3VFDDB	Top Secret	No	IT: N/A Public Trust: N/A Child Care: N/A	Access Number: N/A	Indoctrinate Non-SCI Debrief Non-SCI Indoctrinate SCI Request SPA
Industry (Contractor) 7N699-I		No	IT: N/A Public Trust: N/A Child Care: N/A	Access Number: N/A	
Industry (Contractor) 0S482-I	Top Secret	No	IT: N/A Public Trust: N/A Child Care: N/A	SI TK G B HCS Access Number: B-390000017	Indoctrinate Non-SCI Debrief Non-SCI Indoctrinate SCI Debrief SCI Request SPA
Reserve - Officer (USAF)	Top Secret	No	IT: N/A Public Trust: N/A Child Care: N/A	SI TK G HCS Access Number: N/A	Indoctrinate Non-SCI Debrief Non-SCI Indoctrinate SCI Debrief SCI Request SPA

- A list will appear containing all the “accesses” for which the person is currently indoctrinated.

Figure 29: Debrief SCI Access screen

?







Debrief SCI Access

FISHER, JENNIFER

SSN: 000-02-0728

Grade: O4

Category: Warrant Officer (Guard) (DOD)

	Indoc Date	Debrief Date	Reason for Debrief
SI:	2000 09 22	<input type="text"/> 	<input type="text"/> 
TK:	2000 09 22	<input type="text"/> 	<input type="text"/> 
NK:	2000 09 22	<input type="text"/> 	<input type="text"/> 

Save

Cancel

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

10. Enter a **Debrief Date** and select a **Reason for Debrief** from the drop down box. If you do not select a reason for the debriefing, you will receive a dialog box indicating the system will not perform the debriefing.
11. Click the gray **Save** button and the access is removed.
12. Click on the gray **Cancel** button and it will return you to the person's Person Summary screen.
13. Make sure you have the correct industry category showing in the **Person Category** section. If not, click on the drop down, scroll down and highlight the correct category.
14. Under the **SCI** column in the **Accesses** section, you will see that the person no longer has any accesses. (Figure 28)

Section 10 – How to Out-Process (Removal from PSM Net)

Introduction

When a person is no longer assigned to your SMO, you will need to “debrief” them from any access(es) then “out-process” them from your SMO.

NOTE: If you are a defense contractor, you will also be required to enter a separation date for the person who is terminating from your company. Section 11 describes this process.

There are two ways in which you can “out-process” a person. The first is by selecting the person by their SSN and then using the “in/out process” hyperlink from the Person Summary screen. The second way is to out-process them through your PSM Net. Both ways work about the same, but if you have several people to out-process, then using the PSM Net method would be easier.

The first method we will discuss involves using the “Select Person” method.

Instructions (Person Summary Method)

1. Log in as a **User for the SMO that is losing the person being out-processed.**
2. Click on **Select Person** (column on left).
3. Enter the person’s **SSN**.
4. Click the **Display Person Summary** radio button.
5. Click the gray **Display** button.
6. Make sure the correct category is displayed in the **Person Category** text box (Figure 30). If not, click on the drop down menu and highlight the correct category.

Figure 30: Person Summary screen

Person Summary

RED, ERIC A

Person Category

Active Duty - Enlisted (USAF)

SSN: 995-97-6810

Open Investigation: N/A

PSQ Sent Date: N/A

Attestation Date: 1999 06 18

Incident Report: N/A

SF 713 Fin Consent Date: N/A

SF 714 Fin Disclosure Date: N/A

Polygraph: N/A

Foreign Relation: N/A

Date of Birth: 1972 07 22

Marital Status: N/A

Place of Birth: Maine

Citizenship: U.S. Citizen

NdA Signed: Yes

NdS Signed: Yes

Accesses

Category	US Access	NATO Access	PSP	Suitability and Trustworthiness	SCI
Active Duty - Enlisted (USAF)	Top Secret	NATO S	No	IT: N/A Public Trust: N/A Child Care: N/A	SI TK G HCS

Access Numbers: N/A

Person Category Information

Category Classification: N/A

Organization: EEDUFHGC, 25 INFO OPNS SQ, Hurlburt Field, Hurlburt Field, FL, 32544

Organization Status: N/A

Occupation Code: K1AB51E

SCI SMO: N/A

Separation Date: 2007 01 11

Person Category Information

Category Classification: N/A

Organization: EEDUFHGC, 25 INFO OPNS SQ, Hurlburt Field, Hurlburt Field, FL, 32544

Organization Status: N/A

Occupation Code: K1AB51E

SCI SMO: N/A

Non-SCI SMO: N/A

Servicing SMO: Yes

Office Symbol: DOT

Position Code: N/A

Arrival Date: 2002 10 09

Office Phone Comm: N/A

Separation Status: N/A

Interim: N/A

Grade: ES

PS: N/A

RNLTD: N/A

Office Phone DSR: N/A

TAFMSD: 1992 05 26

Proj. Departure Date: N/A

UNC/RUC/PASCODE: N/A

Report Incident

In/Out Process

Investigation Summary

SBPR from DSS, Opened: 1999 12 28 Closed: 2001 03 20

SSBI from DSS, Opened: 1992 12 23 Closed: 1992 12 23

Adjudication Summary

PSI Adjudication of SBPR DSS, Opened 1999 12 28, Closed 2001 03 20, determined Eligibility of SCI - DCID 6/4 on 2001 05 22

AFCAL

PSI Adjudication of SBPR DSS, Opened 1999 12 28, Closed 2001 03 20, determined Eligibility of SCI - DCID 6/4 on 2001 05 22

AFCAL

External Interfaces

Perform SB Search

DCB

Notice:

Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoD 5400.11, DoD 5400.11-R and the applicable service directives.

- Click the **In/Out Process** hyperlink and the View/Modify In/Out Screen will populate. (Figure 31)

Page 57 of 107

Figure 31: View/Modify In/Out screen

View/Modify In/Out

HILL, JOHN S

SSN:

Grade: GS

Category: Civilian Employee (DOD)

Owning SCI SMO: N/A

Owning Non-SCI SMO: DSSHQSEC - DEFENSE SECURITY SERVICE, HEADQUARTERS SECURITY, Level 4, 703-325-9458/9638,

Add New Relationship

* SMO: DSSTEST - DEFENSE SECURITY SERVICE, SETA, TEST, Level 3

Select SMO

* In Date:

* Out Date:

* Relationship: ☐ Owning ☐ Servicing

View/Modify Active Relationship(s)

Code	Name	Location	Level	In Date	Out Date	Relationship	Change
DSSAPS6	DEFENSE SECURITY SERVICE, DSSA	LINTHICUM, MD	Level 6	2005 05 05	N/A	Servicing	<div>Reason</div>
DSSHQSEC	DEFENSE SECURITY SERVICE, HEADQUARTERS SECURITY	ALEXANDRIA, VA	Level 4	2003 01 10	N/A	Owning	<div>Reason</div>
DSSTEST	DEFENSE SECURITY SERVICE, SETA, TEST	LINTHICUM, MD	Level 3	2005 07 13	<div></div>	Servicing	<input type="checkbox"/>

Save

Cancel

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

Print Screen 8-2

- Enter the date (Format: YYYY MM DD) in the **Out Date** box under the **View/Modify Active Relationship** section or click on the **calendar** and choose the appropriate date.
- Click on the gray **Save** button and the screen will refresh with the out-process date appearing solid.
- Click on the gray **Cancel** button and it will take you back to the Person Summary screen.
- Now if you click on your **PSM Net** and lookup that person, the phrase “Pending Removal” will appear under the **Remove** heading in the far right column. (Figure 32) The system will update at midnight EST and the “Pending Removal” notation will be removed.

Figure 32: JCAVS Maintain PSM Net screen

JCAVS Maintain PSM Net

***SMO:** EDSSUPRT2 - EDS JPAS SUPPORT OFFICE, Level 2

Select SMO

☐ Person Categories by Organization
 ☐ Person Categories by SSN

Add

Person Categories by Organization

Remove

Person Categories:

Records 1 - 23 of 23, Page 1 of 1

SSN	Name	Category	Organization	Relationship	Change	Remove
000-00-2221	BROCCOLI, NICHOLAS A	DoD Civilian/Reserve/National Guard	0106 RESCUE WG	Servicing	<input type="checkbox"/>	<div>Pending Removal</div>
000-00-8227	BUCK, JASON A	Active Duty	0001 SPACE LAUNCH SQ	Servicing	<input type="checkbox"/>	<input type="checkbox"/>
000-00-2237	CLARK, TREVOR M	Industry	EG&G TECHNICAL SERVICES, INC.	Servicing	<input type="checkbox"/>	<input type="checkbox"/>
000-00-8220	HANSEN, BRUCE EDWARD	Industry	HNC SOFTWARE, LLC	Servicing	<input type="checkbox"/>	<input type="checkbox"/>
000-00-6022	HYATT, SHANNON K	Active Duty	0033 AIRCRAFT MAINT SQ	Owning	<input type="checkbox"/>	<input type="checkbox"/>
000-00-7422	JOLES, DONALD MARK	Industry	AERO SYSTEMS CE	Owning	<input type="checkbox"/>	<input type="checkbox"/>
000-00-7564	KROPP, GREGORY A	Reserve	0093 BOMB SQ	Owning	<input type="checkbox"/>	<input type="checkbox"/>
000-00-2877	LAVALLEY, MIKKO R	Active Duty	0086 OPERATIONS GP	Servicing	<input type="checkbox"/>	<input type="checkbox"/>
000-00-3212	LINGELBACH, JOHN EDWARD	Civilian Employee	TTW8A0AA	Servicing	<input type="checkbox"/>	<input type="checkbox"/>
000-00-3444	LINGELBACH, JOHN EDWARD	DoD Civilian/Reserve/National Guard	HQ STARC IA ARNG	Servicing	<input type="checkbox"/>	<input type="checkbox"/>
000-00-3727	LINGELBACH, JOHN EDWARD	National Guard	TRP A 1ST SQDN 113TH CAV	Servicing	<input type="checkbox"/>	<input type="checkbox"/>
000-00-8879	MCCAIN, GAIL	Active Duty	0056 MEDICAL OPERATIONS SQ	Servicing	<div>Reason</div>	<input type="checkbox"/>
000-00-2567	PARCHMENT JR, EARL W	Industry	CRESTVIEW AEROSPACE CORPORATIO	Servicing	<input type="checkbox"/>	<input type="checkbox"/>
000-00-1099	PASSARELLO, STEPHEN M	Civilian Employee	ARNOLD ENGR DEV CE	Servicing	<input type="checkbox"/>	<input type="checkbox"/>
000-00-1546	SICK, JEFFREY R	Active Duty	AFELM USCENTCOM JD	Servicing	<input type="checkbox"/>	<input type="checkbox"/>
000-00-0547	SPOSITO, CHRISTOPHER MICHAEL	National Guard	227TH MI CO	Servicing	<input type="checkbox"/>	<input type="checkbox"/>
000-00-0998	SWIESZCZ, MARK R	Active Duty	0437 CIVIL ENGINEER SQ	Owning	<input type="checkbox"/>	<input type="checkbox"/>
000-00-3566	THOMASSON, WAYNE ANTHONY	Reserve	N/A	Servicing	<input type="checkbox"/>	<input type="checkbox"/>
000-00-2441	TOWNSEND, JOHN D	Active Duty	N/A	Servicing	<input type="checkbox"/>	<input type="checkbox"/>
000-00-4123	VANDERSLUIS, MARK STUART	Industry	N/A	Servicing	<input type="checkbox"/>	<input type="checkbox"/>
000-00-8987	WITT, RICHARD D	Civilian Employee	USAR CENTER	Servicing	<input type="checkbox"/>	<input type="checkbox"/>
000-00-8654	WITT, RICHARD D	Reserve	FT LEONARD WOOD USAR CENTER	Servicing	<input type="checkbox"/>	<input type="checkbox"/>
000-00-9344	YUTZEY, KATHERINE A	Reserve	N/A	Servicing	<input type="checkbox"/>	<input type="checkbox"/>

Save

Cancel

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

Instructions (PSM Net Method)

1. Log in as a **User for the SMO that is losing the person being out-processed.**
2. Click on **PSM Net** (column on left).
3. Locate the **Person Categories** within your PSM Net.
4. Click on the far right **check box** under the **Remove** column.
5. Click the gray **Save** button at the bottom of the page. When the screen refreshes, you will see “Pending Removal” under the **Remove** column for the person you want to remove. The system will update at midnight EST and the “Pending Removal” notation will be removed.

Section 11 – How to Enter a Separation Date (Industry Only)

Introduction

Separation Date Text Box: Enter the separation date for a Person in the YYYY MM DD or YYYYMMDD format. An entry in this field requires a Separation Code selection from the **Separation Code** drop-down menu.

NOTE: This date will serve as the date the person category is to be "separated" from JPAS.

Separation Code Drop-Down Menu: Highlight and select the appropriate Separation Code for the Person. An entry in this field requires a Separation Date entry in the **Separation Date** field.

Instructions

1. Log in as a **User for the SMO for the employee you are separating**.
2. Click on **Select Person** (column on left).
3. Enter person's **SSN**.
4. Click the **Display Add/Modify Non-DoD Person** radio button.
5. Click the gray **Display** button.
6. The Display Add/Modify Non-DoD Person screen appears (Figure 33a).
7. Make sure the correct Organization code is listed in the **Person Category** text box. If not, click on the drop down menu and highlight the correct Organization code.

Figure 33a: Add/Modify Non-DoD Person screen

?

Add/Modify Non-DoD Person

SSN: 000-02-1026

*Last Name: NO CATS

*First Name: PERSON

Middle Name: 130181135

Cadency: sufx

*DOB: 1967 01 25

*Citizenship: A - U.S. Citizen

Date of Death:

State of Birth: Wisconsin

*Country of Birth: US - United States Of America

Eligibility: Interim SCI, , ArmyCCF

Investigation: N/A

Open Investigation: N/A

Incident Report: N/A

Polygraph: N/A

Foreign Relation: N/A

Modify Relationship

Available Category Types: Industry 2

Add Category

Person Category: Industry ()

Position:

Category

Classification: (Required for Industry Categories only)

Separation Date:

Separation Code:

Organization/Company/Agency

Modify Organization

Name: N/A

Location: N/A

Person Summary

Save

Cancel

Notice:

Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

8. Enter a date in the **Separation Date** text box. (Figure 33b)

NOTE: You can enter the actual date the person separated with the organization or you can use the current date.

9. Click on the **Separation Code** drop down menu; highlight the appropriate reason code.

Figure 33b: Add/Modify Non-DoD Person screen

?

Add/Modify Non-DoD Person

SSN: 000-02-1026

*Last Name: NO CATS

*First Name: PERSON

Middle Name: 130181135

Cadency: sufx

*DOB: 1967 01 25

*Citizenship: A - U.S. Citizen

Date of Death:

State of Birth: Wisconsin

*Country of Birth: US - United States Of America

Eligibility: Interim SCI, , ArmyCCF

Investigation: N/A

Open Investigation: N/A

Incident Report: N/A

Polygraph: N/A

Foreign Relation: N/A

Modify Relationship

Available Category Types: Industry 2

Add Category

Person Category: Industry ()

Position:

Category

Classification: (Required for Industry Categories only)

Separation Date:

Separation Code:

Organization/Company/Agency

Name: N/A

Location: N/A

Modify Organization

Person Summary

Save

Cancel

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

10. Click the gray **Save** button.

Page 63 of 107

Section 12 – How to Document “PSQ Sent”

Introduction

Whenever you submit a PSQ to the appropriate CAF for any reason (e.g., new eligibility or Periodic Reinvestigation, etc.), you will be required to document in JPAS the fact that the PSQ was sent. This action can only be performed on a person in your PSM-Net

Instructions

1. Log in as a User for **the SMO for the person for whom you are submitting the PSQ.**
2. Click on **Select Person** (column on left).
3. Enter the person’s SSN.
4. Click the **Display Person Summary** radio button.
5. Click the gray **Display** button.
6. The person’s Personal Summary screen should appear with the person’s name printed at the top. (Figure 34)
7. Click on the **PSQ Sent** hyperlink.

Figure 34: Personnel Summary screen

Person Summary

HARBACK, HELEN K

Person Category

Industry (Contractor) HH3VFDDB

SSN: 926-60-5777

Open Investigation: N/A

PSQ Sent Date: N/A

Attestation Date: N/A

Incident Report: N/A

SF 713 Fin Consent Date: N/A

SF 714 Fin Disclosure Date: N/A

Polygraph: N/A

Foreign Relation: N/A

PSQ Sent

Non-SCI Access History

Unofficial Foreign Travel

NdS History

Date of Birth: 1966 05 17

Marital Status: N/A

Place of Birth: New York

Citizenship: U.S. Citizen

NdA Signed: Yes

NdS Signed: Yes

SCI Access History

Request to Research/Upgrade Eligibility

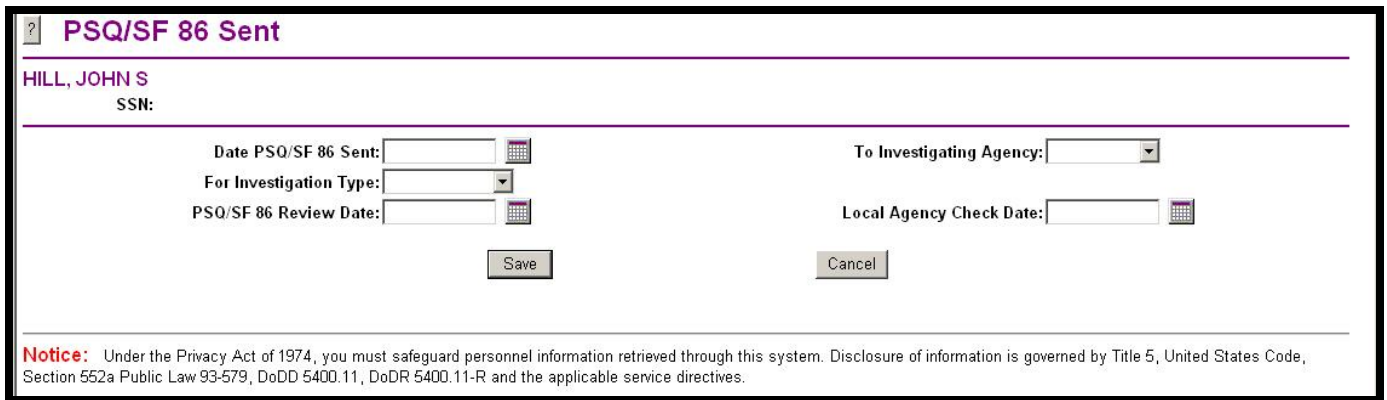
NdA History

Accesses

Category	US Access	PSP	Suitability and Trustworthiness	SCI	Available Actions
Industry (Contractor) HH3VFDDB	Top Secret	No	IT: N/A Public Trust: N/A Child Care: N/A	Access Number: N/A	Indoctrinate Non-SCI Debrief Non-SCI Indoctrinate SCI Request SPA
Industry (Contractor) 7N699-I		No	IT: N/A Public Trust: N/A Child Care: N/A	Access Number: N/A	
Industry (Contractor) 0S482-I	Top Secret	No	IT: N/A	SI	Indoctrinate Non-SCI


Page 64 of 107

Figure 35: PSQ/SF 86 Sent screen




? PSQ/SF 86 Sent


HILL, JOHN S
SSN:

Date PSQ/SF 86 Sent: 

For Investigation Type: ▼

PSQ/SF 86 Review Date: 

To Investigating Agency: ▼

Local Agency Check Date: 

Save Cancel

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

8. The PSQ/SF 86 Sent screen appears (Figure 35).
9. Enter all applicable information (**all** field boxes require an entry prior to submission).
10. Click the gray **Save** button.

NOTE: The PSQ sent date will now be populated in the Person Summary screen.

Section 13 - JCAVS Interface with e-QIP

The Electronic Questionnaires for Investigations Processing system (e-QIP) is part of an e-government initiative sponsored by the Office of Personnel Management (OPM). e-QIP allows applicants to electronically enter, update, and transmit their personal investigative data over a secure Internet connection to their employing agency or security management office for review and approval of the personnel security investigation request.

The e-QIP is accessible from a secure website at www.opm.gov/e-QIP that is designed to house all personnel security investigative forms.

Through an interface with the Joint Clearance Access and Verification System (JCAVS), e-QIP allows authorized requesters to electronically transmit requests for investigation (SF 86) electronically versus mailing. Authorized requestors must be a JCAVS user at level 2, 3, 4, 5 or 6 and have requester permission granted by the account manager for their Security Management Office (SMO).

e-QIP replaced the Electronic Personnel Security Questionnaire (EPSQ). e-QIP can be accessed at www.opm.gov/e-QIP.

How do you get permission to use the JCAVS interface with e-QIP?

Current account managers will be able to grant the permissions described below in JCAVS:

Initiate PSI - permission to Initiate an Investigation Request for a person.

Review PSQ - permission to Review a PSQ for a person having an active Investigation Request.

Approve PSQ - permission to Approve an Investigation Request for a person.
(DISCO is the approver for Industry users.)

Override PSQ - permission to override an Investigation Request for a person. (Level 2 and 4 Users only)

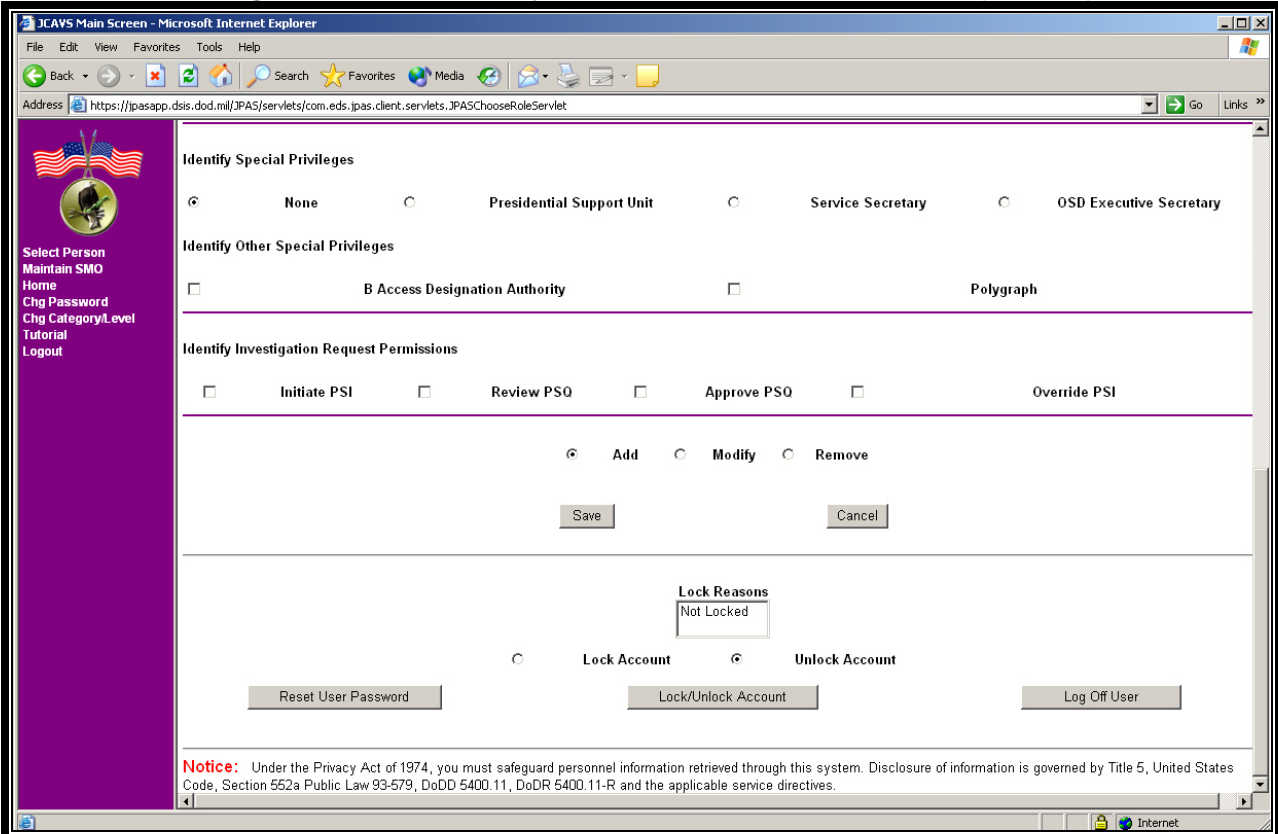
The assignment of these permissions is based on the following roles:

New Users: Request permissions based on your organization's needs.

Previous Users: Permissions can be updated by your account manager.

Account Managers: If you are the only account manager at your location, contact the account manager at next level in your command. Industry users contact the DoD Security Services Center. Alternate Account managers may grant you the permission. (Account managers do not need to have e-QIP permissions to grant permissions.) See Section 3 - **Account Manager Functions**

Figure 12b: Add/Modify/Remove JCAVS Users screen (bottom)



JCAVS Main Screen - Microsoft Internet Explorer

Address: <https://jpasapp.dsis.dod.mil/JPAS/servlets/com.eds.jpas.client.servlets.JPASChooseRoleServlet>

Identify Special Privileges

☒ None ☐ Presidential Support Unit ☐ Service Secretary ☐ OSD Executive Secretary

Identify Other Special Privileges

☐ B Access Designation Authority ☐ Polygraph

Identify Investigation Request Permissions

☐ Initiate PSI ☐ Review PSQ ☐ Approve PSQ ☐ Override PSI

☒ Add ☐ Modify ☐ Remove

Save Cancel

Lock Reasons

Not Locked

☐ Lock Account ☒ Unlock Account

Reset User Password Lock/Unlock Account Log Off User

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

Other Pre-requisites

Before processing an individual for a personnel security investigation (PSI) using e-QIP, the following requirements must be met:

- Person Category must be “active.”
- Person Category must not have “access suspended.”
- Person must not be in “Due Process.”
- Person must not already have an active PSI request.
- Person Category must be in the requester’s Personnel Security Management Network (PSMNET) with an owning or servicing relationship.
- For Industry – “DoD Contractor Companies” must be listed in all Service Agency boxes throughout the system.

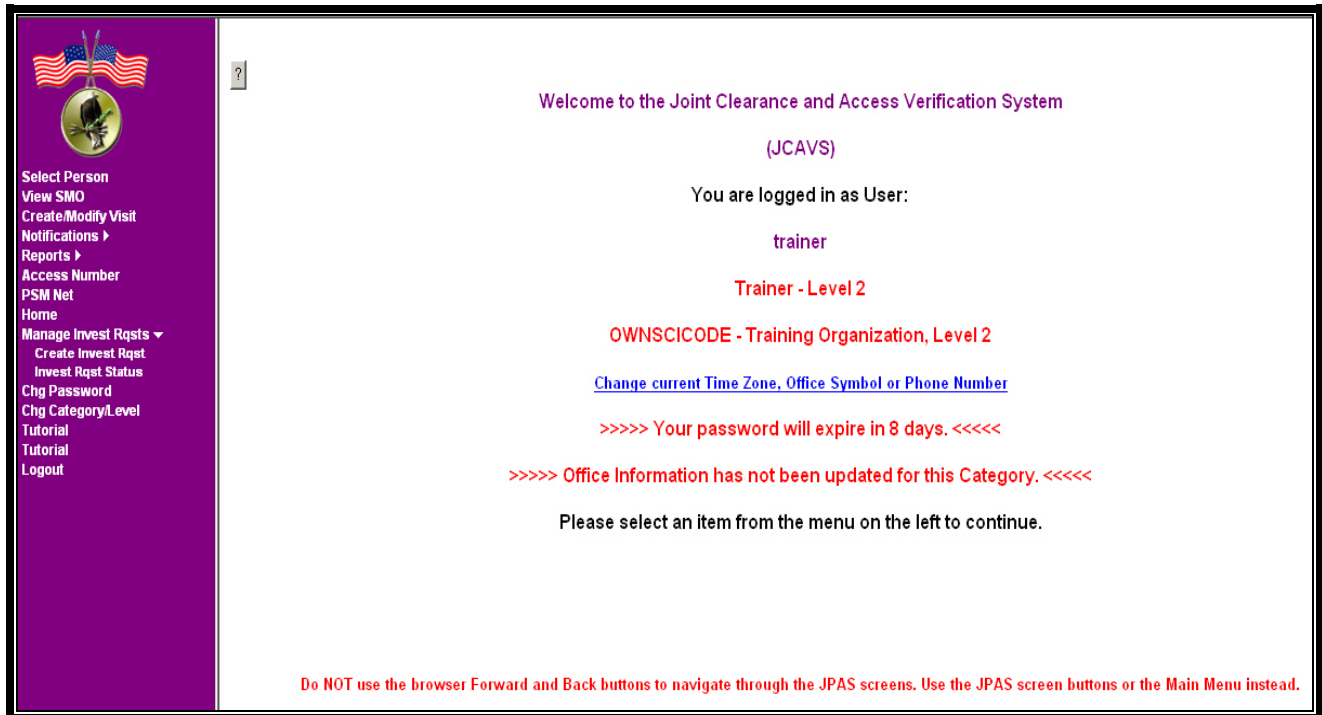
If the person has been “Denied” or “Revoked” eligibility, that decision must be older than 12 months. The date of the denial/revocation will be on the Person Summary screen on the “Eligibility” line, as well as under the “Adjudication Summary” section of the screen.

How do you initiate an investigation in JCAVS?

The Authorized Requester will access the **Investigation Request** function via the **JCAVS Person Summary** screen:


1. On Main Menu, Click the **Manage Invest Rqsts** link, the **Create Invest Rqst** and **Invest Rqst Status** links will appear.

Figure 5: JCAVS Welcome screen and Main Menu



2. Click the **Create Invest Rqsts** link. The Select Person screen will appear.

Figure 7: Select Person screen

 **Select Person**

*SSN:

Last Name:

First Name:

Middle Name:

Display Person Summary: ☒

Display abbrev. Person Summary with VISIT Info: ☐

Display Add/Modify Non-DoD Person: ☐

Display SII: ☐


Display

Clear

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

2. Enter person's SSN, ensure the **Display Person Summary** radio button is selected
3. Click the gray **Display** button. The Person Summary screen will display. If the person has multiple categories, click on the **Person Category** drop-down menu and select the appropriate person category.
4. Scroll down to **Person Category Information** section

Figure 8a: Person Summary screen (middle)



Select Person
View SMO
Create/Modify Visit
Notifications >
Reports >
Access Number
PSM Net
Home
Manage Invest Rqsts >
Create Invest Rqst
Invest Rqst Status
Chg Password
Chg Category/Level
Tutorial
Tutorial
Logout

(This training application only allows a view of 1 Category in the Access section)

--	--	--	--	--

Person Category Information

Category Classification: N/A
Organization: N/A
Occupation Code: 14NX
SA: N/A
Arrival Date: 2005 01 01
[Office Phone Comm:](#) 456-4567
Separation Date: N/A
Separation Status: N/A
Interim: Interim Confidential, 2003 02 15
PSP: Yes
SCI SMO: PS123.01 - JPAS/JCAVS Training for Security Professional, Level 2 410-823-4759, us@dss.mil
Non-SCI SMO: SITE SUPPORT GREEN BAY, Level 4, 801-601-1111, site.support@eds.com

[Report Incident](#)
[PSP Decision](#)
[Suspense Data](#)

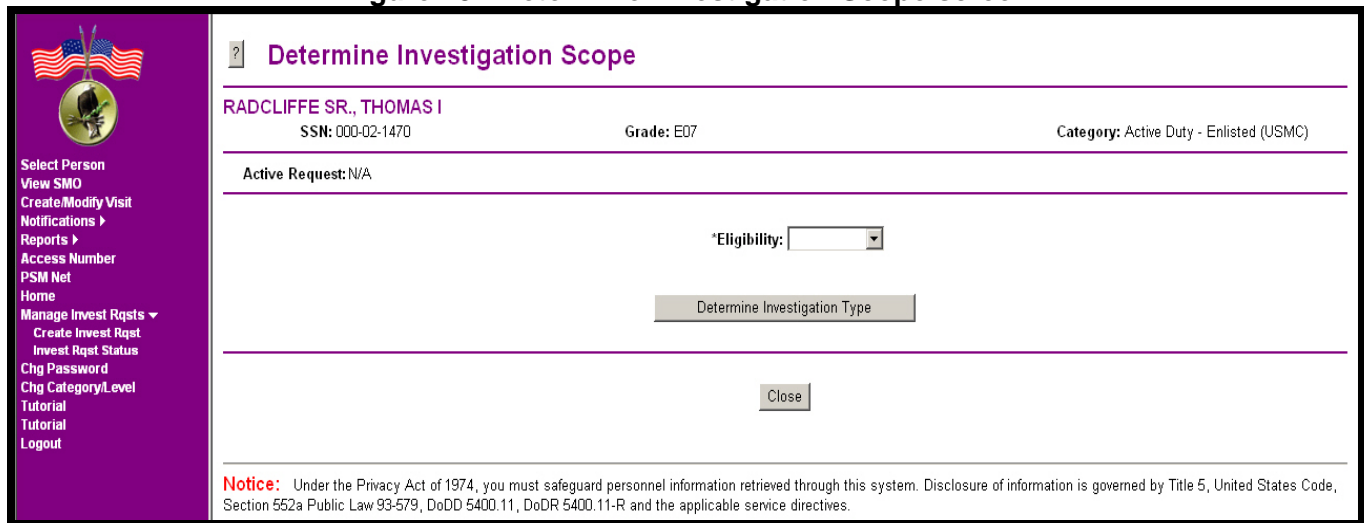
[In/Out Process](#)
[Remove From PSP](#)
[Investigation Request](#)

[Request Indoc/Debrief Assistance](#)
[Remarks](#)

[Office Symbol:](#) ABCD
Grade: 04
PS: Non Sensitive
[Office Phone DSN:](#) (301) 604-5600
RNLTD: 2000 09 22
TAFMSD: 2000 09 22
Proj. Departure Date: N/A
Proj. UIC/RUC/PASCODE: N/A

- Click the **Investigation Request** link, the Determine Investigation Scope screen will appear.

Figure 43: Determine Investigation Scope screen



Determine Investigation Scope

RADCLIFFE SR., THOMAS I
SSN: 000-02-1470 Grade: E07 Category: Active Duty - Enlisted (USMC)

Active Request: N/A

*Eligibility:

Determine Investigation Type

Close

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

- Select eligibility type from **Eligibility** drop down Menu.

Note: For Industry SSNs, you will need to enter a number in the **Prime Contract Number** field. The field is required for Industry SSNs but is not shown on the screen capture above.


- Click the gray **Determine Investigation Type** box, the Determine Investigation Scope screen appears. Under the *Initiation Scope* section, the “Recommended Investigation Type” will populate based upon the Eligibility selected. Level 2 and 4 JCAVS users with the override permission can change the Investigation Type and enter an Override Justification. “Sensitivity Level Code” will populate based on the Category of the selected member.

Industry – Sensitivity = Industry

DoD Civilian - Sensitivity = Sensitive/critical sensitive/special

Military – Sensitivity = Military

Figure 43a: Determine Investigation Scope Initiation Scope Screen



- Select Person
- View SMO
- Create/Modify Visit
- Notifications ▶
- Reports ▶
- Access Number
- PSM Net
- Home
- Manage Invest Rqsts ▼
 - Create Invest Rqst
 - Invest Rqst Status
- Chg Password
- Chg Category/Level
- Tutorial
- Tutorial
- Logout

Determine Investigation Scope

RADCLIFFE SR., THOMAS I
SSN: 000-02-1470
Grade: E07
Category: Active Duty - Enlisted (USMC)

Active Request: N/A

*Eligibility: Secret

Determine Investigation Type

Initiation Scope

Eligibility: Secret

Recommended Investigation Type: SSBI
*Investigation Type: SSBI
Override Justification:

*Sensitivity Level Code: Military

*Duty/Position Code:

Periodic Reinvestigation: No

Recommended Service Code:
*Service Code:
Override Justification:

OK
Cancel


Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

8. The **Duty/Position Code**. Duty Position Code is no longer required.

The “Recommended Service Code” will populate based on the **Category and Investigation Scope** selected. Level 2 and 4 JCAVS users with the override permission can change the “Service Code” and enter an “Override Justification”. (Industry users cannot override this field.)

9. Click **OK** when complete. After clicking the **OK** button on the Determine Investigation Scope screen, the Add/Modify Investigation Request screen will appear.

Figure 43b: Add/Modify Investigation Request screen



- Select Person
- View SMO
- Create/Modify Visit
- Notifications ▶
- Reports ▶
- Access Number
- PSM Net
- Home
- Manage Invest Rqsts ▼
 - Create Invest Rqst
 - Invest Rqst Status
- Chg Password
- Chg Category/Level
- Tutorial
- Tutorial
- Logout

Add/Modify Investigation Request

RADCLIFFE SR., THOMAS I
SSN: 000-02-1470
Grade: E07
Category: Active Duty - Enlisted (USMC)



Active Request: N/A

Investigation Scope

Investigation Type: SSBI
Periodic Reinvestigation: No
Sensitivity Level Code: Military
Duty Position Code: Special/Confidential Assistants (GS/GM-13 and above)
Service Code: 120 days

Scope Detail

Additional Scope Information

*Form Type: SF-86
*Date of Birth: 
Advance NAC Extra Coverage: ☐
*Local Agency Check Date: 
*Service Agency: Marines
SOL: NV00
*OPAC-ALC: DoD-MC

*Position Title: Military
*Access Code:
Sensitivity ADP:

SON: N999

10. On the Add/Modify Investigation Request screen, you can update scope detail by clicking the gray **Scope Detail** box and/or completing the *Additional Scope Information*, *Additional Request Information* and/or *Investigation Request Status History* sections.
11. **Form Type** is pre-populated because the SF Form 86 is the only option currently available.
12. **Position Title** will pre-populate based on the Person Category.
13. **Date of Birth** usually pre-populates. If not, use the Calendar widget to select the correct Date of Birth.
14. Select the appropriate access required from the **Access Code** drop down menu. For Military members this is based on the Command Local Access requirements. For Industry this is based on the DD254.
15. Check the **Advance NAC Extra Coverage** box, if required for an interim determination. DISCO makes interim determinations for Industry.
16. Select **Sensitivity ADP**, if required, from the **Sensitivity ADP** drop down menu.
17. Enter **Local Agency Check Date**. Use the calendar widget to enter the date of any local records checked.
18. **Service Agency** is usually pre-populated. Users may choose the appropriate service agency when the person's service agency does not have an associated OPAC/ALC, or SOI.
19. **(SOI) - Security Office Identifier** - pre-populates based on the Subject's Person Category and Service Agency.
20. **(SON) - Submitting Office Number** - is the billing code used by OPM. Department of Defense (DoD) users should check their component policy and procedures to enter the appropriate DoD SON. Industry users should enter **346W**.
21. **(OPAC-ALC) - On Line Payment and Collection Agency Locator Code** - usually pre-populates with Agency information based on the Service Agency and is required for billing purposes. If you are an industry user, your OPAC-ALC code will always be **DSS-IND**.
22. Complete the **Additional Request Information** section.

Figure 43c: Add/Modify Investigation Request screen (bottom)

Additional Request Information

Requesting Official

*Name:

Title:

*Phone Number: Extension:

Security Folder

*Location:

Location Name:

Street Address 1:

Street Address 2:

Street Address 3:

City:

State: Zip Code:

Official Personnel Folder

*Location:

Location Name:

Street Address 1:

Street Address 2:

Street Address 3:

City:

State: Zip Code:

Investigation Request Status History

☐ Pending PSI ☐ Initiate PSI

23. Enter the Requesting Official's **name**, **title** and **commercial phone** number (NO DSN).
24. Select the **Location** of the Security Folder from the drop down menu. Select **None**, if one is not established. Other options are **NPI** - No pertinent Information, **Other** - Enter the Location Name and Street Address, or **SOI** - Security Office Identifier.
Note: For Industry SSNs, this information is pre-populated.
25. Select the **Location** of the Official Personnel Folder from the drop down menu. Check only one box. For military personnel with no prior civilian Federal service, check **None**.
26. If you are not ready to have the applicant begin completing his/her PSQ, e.g., the applicant is out of town for an extended period, select the **Pending PSI** radio button and click the **Save** button.
27. If you are ready to have the applicant begin completing his/her PSQ, select the **Initiate PSI** radio button and click **Save** or **Save and Return**.

Contact the Applicant and advise him/her to log in to www.opm.gov/e-qip.

Asterisks (*) on the screen capture indicate required fields.

What are the timelines when initiating, reviewing and approving an e-QIP submission?

Initiating

30 Days: Once an Investigation Request is initiated in JPAS, an applicant has 30 days to login to e-QIP and start their PSQ (personnel security questionnaire) or the Investigation Request is terminated.

90 Days: Once an Investigation Request is initiated in JPAS, the applicant has 90 days after their initial e-QIP login date to complete their PSQ or the Investigation Request is terminated.

Reviewing and Approving

90 Days: Once the applicant has completed the PSQ, it must be reviewed and approved by the appropriate agency within 90 days or the Investigation Request is terminated.

What are some other important e-QIP timelines?

Pending PSQs

30 Days: An Investigation Request that remains in a Pending Status and is not “Initiated” will be deleted 30 days after creation.

Stopped PSQs

90 Days: If an applicant has begun their PSQ, but the Investigation Request was stopped, it must be resumed within 90 days.

30 Days: If the applicant has not begun their PSQ, but the Investigation Request was stopped, it must be resumed within 30 days.

Revised PSQs

60 Days: An applicant has 60 days to login to e-QIP and complete updates to their PSQ if revisions are required.

Facility Notifications

15 Days: An Investigation Request must be ready to be reviewed 15 days after initiation for an active Person Category with Key Management Personnel (KMP) category classification in a Facility with a status of “In Process” or a Facility Notification will be generated.

How to Review and Approve an e-QIP Submission

Reviewer/Approver must be a JCAVS User level 2, 3, 4, 5, 6 with permissions granted.

Reviewer/Approver must be in the initiating JCAVS SMO.

JPAS notifies the initiating SMO through JCAVS notifications that the investigation request is ready for review.

The SMO is also notified of each subsequent status change, e.g., approved, revise, stopped, etc.

Investigation Request Status Notifications are not removed by the system and must be manually removed. You must click **Remove From Display** and then **Save**.

The JCAVS requester can access the **Add/Modify Investigation Request** screen to review and approve the investigation request.

The JCAVS **Person Summary Investigation Summary** case line also displays Investigation Request status.

Industry: Initiating SMO can electronically Review the e-QIP. DISCO is the final approver; you will get a message via “Message from CAF” if a process is stopped and the reason why.

After the Subject enters his/her Personnel Security Questionnaire (PSQ) in e-QIP and JPAS receives confirmation of this action from e-QIP, the **Investigation Request Status Notification** is created.

Process

To view the questionnaire, click **View PSQ**.

You can either view the questionnaire “on-line” or “print it.” (PDF format)

To view the Subject’s release forms, click **View Signature Forms**.

The forms must be signed and dated and mailed to OPM.

At this point you can **Review**, **Review and Approve**, **Revise**, or **Stop** the PSQ based on the permissions you were granted by your account manager.

The JPAS notification reflects status of submitted questionnaire.

Review

1. Select **Invest Rqst Status** from the menu. The Investigation Request Status Notification Screen will appear. This screen will display Investigation Requests for a single SMO. Active requests (Pending, Initiated, Ready for Review and Ready for Approval) will always display. Inactive requests (Approved, Revised, Terminated and Stopped) will be removed from display by the user or systematically removed through a parameter set in JPAS.


Figure 5: JCAVS Welcome screen and Main Menu

Figure 44: JCAVS Investigation Request Status Notification screen and Main Menu

SSN	Name	Category	Investigation Type	Status	Status Change Date	Days Until Termination	Remove From Display
000-81-3211	GRAMM, GIA SARAH	Active Duty	SSBI	Ready for Review PSQ	2004 03 20	25	<input type="checkbox"/>
123-45-6789	MAG-OO, THEODORE S	Warrant Officer (Reserve)	ANCI	Initiated PSI	2004 02 06	20	<input type="checkbox"/>
000-10-1694	ZEME, GIA PEG	Active Duty	NACI	Terminated PSI	2004 03 15	N/A	<input type="checkbox"/>
000-87-5330	CAGLE, INEZ MADISON	Active Duty	SSBI	Ready for Approval PSQ	2004 10 02	15	<input type="checkbox"/>
		Academy	NLC	Approved PSQ	2004 05 25	N/A	<input type="checkbox"/>

2. Click on the **Ready for Review PSQ** link for the applicable name of the record you plan to review. The Add/Modify Investigation Request screen will appear.
3. Scroll down to bottom portion of screen.

Figure 43d: Add/Modify Investigation Request with Investigation Request Status History screen (bottom)



- Select Person
- View SMO
- Create/Modify Visit
- Notifications ▾
- Reports ▾
- Access Number
- PSM Net
- Home
- Manage Invest Rqsts ▾
 - Create Invest Rqst
 - Invest Rqst Status
- Chg Password
- Chg Category/Level
- Tutorial
- Tutorial
- Logout

Additional Request Information

Requesting Official
*Name:
Title:
*Phone Number: Extension:

Security Folder
*Location:
Location Name:
Street Address 1:
Street Address 2:
Street Address 3:
City:
State: Zip Code:

Official Personnel Folder
*Location:
Location Name:
Street Address 1:
Street Address 2:
Street Address 3:
City:
State: Zip Code:

Investigation Request Status History

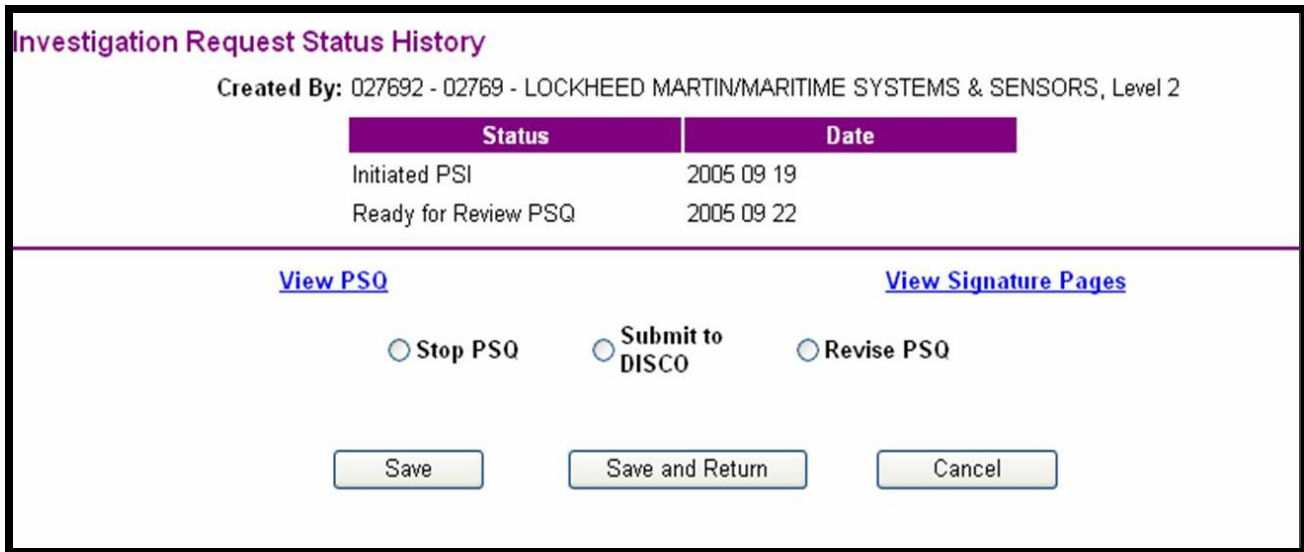
Created By: PS123.01 - JPAS/JCAVS Training for Security Professional, Level 2

Status	Date
Pending PSI	2004 09 18
Initiated PSI	2004 09 19
Initiated PSI (Stopped)	2004 09 20
Initiated PSI (Resumed)	2004 09 21
Ready for Review PSQ	2004 09 22

[View PSQ](#)
[View Signature Page](#)

☐ Review PSQ
☐ Review and Approve PSQ
☐ Revise PSQ
☐ Stop PSQ

Figure 43e: Investigation Request Status History Screen (bottom) Industry



The screenshot shows the 'Investigation Request Status History' screen. At the top, it says 'Created By: 027692 - 02769 - LOCKHEED MARTIN/MARITIME SYSTEMS & SENSORS, Level 2'. Below this is a table with two columns: 'Status' and 'Date'. The table contains two rows: 'Initiated PSI' with date '2005 09 19' and 'Ready for Review PSQ' with date '2005 09 22'. Below the table are two links: 'View PSQ' and 'View Signature Pages'. Under 'View PSQ' are three radio buttons: 'Stop PSQ', 'Submit to DISCO', and 'Revise PSQ'. At the bottom are three buttons: 'Save', 'Save and Return', and 'Cancel'.

Status	Date
Initiated PSI	2005 09 19
Ready for Review PSQ	2005 09 22

[View PSQ](#) [View Signature Pages](#)

☐ Stop PSQ ☐ Submit to DISCO ☐ Revise PSQ

4. Click **View PSQ** link. File will open in another frame as a PDF file.

5. Click **View Signature Page**. File will open in another frame

6. Select **Review** radio button.

Note: If the User has only Review and not Approve, the screen is read-only. If the User has both Review and Approve, the screen is editable and they can review and approve at the same time (by selecting **Review and Approve radio button**).

Industry: If after reviewing PSQ and Signature Pages with no errors you would like to submit to DISCO for Approval, select the **Submit to DISCO** radio button.

7. Click **Save** or **Save and Return** (When you select **Save**, you remain on page. If you select **Save and Return**, you return to previous page. *“Ready for Approval PSQ”* should appear in *Investigation Request Status History* section.

If during review you find errors or items that the applicant needs to update, you can select the **Revise PSQ** radio button. (See **Revise** section for details)

If during review you determine the applicant no longer needs PSI, you can select the **Stop PSQ** radio button (See **Stop** Section for details)

Approve

If a **Ready for Review** or **Ready for Approval** PSQ appears in the **Investigation Request Status History** section and you have permission to approve, you may:

1. Complete **Review** steps 1-5 (above), then
2. Select **Approve** radio button or **Review and Approve** radio button if you have both permissions. The **Approvers Phone** box will appear (for Civilian and Military SSNs only).

Figure 43f: Add/Modify Investigation Request with Investigation Request Status History screen (bottom) Approver

Requesting Official

*Name: Captain John Smith
 Title:
 *Phone Number: (111) 222-3333 Extension:

Security Folder

*Location: At SOI
 Location Name:
 Street Address 1:
 Street Address 2:
 Street Address 3:
 City:
 State: Zip Code:

Official Personnel Folder

*Location: NPRC
 Location Name:
 Street Address 1:
 Street Address 2:
 Street Address 3:
 City:
 State: Zip Code:

Investigation Request Status History

Created By: PS123.01 - JPAS/JCAVS Training for Security Professional, Level 2

Status	Date
Pending PSI	2004 09 18
Initiated PSI	2004 09 19
Initiated PSI (Stopped)	2004 09 20
Initiated PSI (Resumed)	2004 09 21
Ready for Review PSQ	2004 09 22

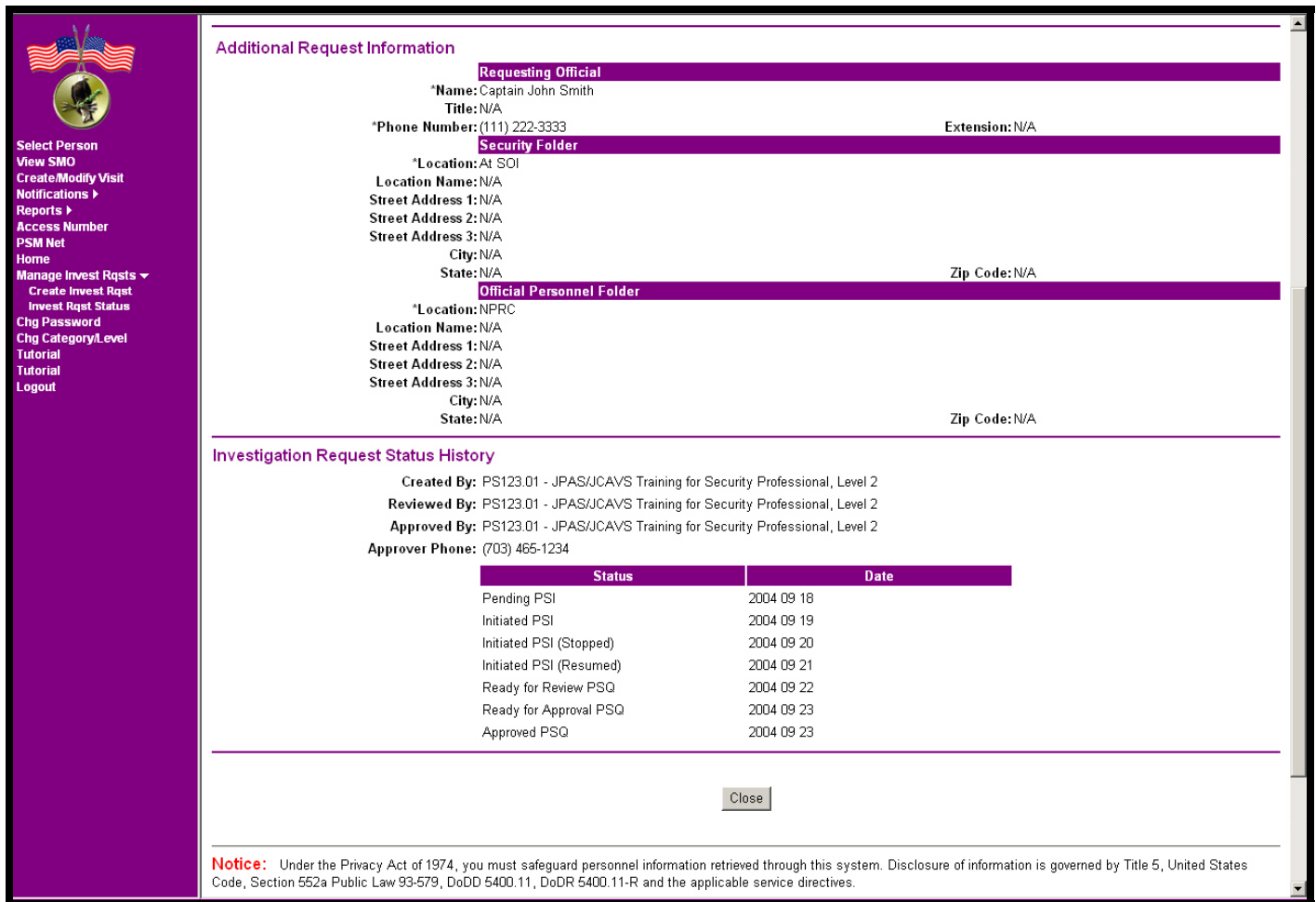
[View PSQ](#) [View Signature Page](#)

☐ Review PSQ
 ☒ Review and Approve PSQ
 ☐ Revise PSQ
 ☐ Stop PSQ

Approver Phone:

3. Input **Approver's Phone** number
4. Click **Save** or **Save and Return**. (When you select **Save**, you remain on the page. If you select **Save and Return**, you return to the previous page.)

Figure 43g “Add/Modify Investigation Request” with Investigation Request Status History” screen (bottom) - Approved



Additional Request Information

Requesting Official
 *Name: Captain John Smith
 Title: N/A
 *Phone Number: (111) 222-3333 Extension: N/A

Security Folder
 *Location: At SOI
 Location Name: N/A
 Street Address 1: N/A
 Street Address 2: N/A
 Street Address 3: N/A
 City: N/A
 State: N/A Zip Code: N/A

Official Personnel Folder
 *Location: NPRC
 Location Name: N/A
 Street Address 1: N/A
 Street Address 2: N/A
 Street Address 3: N/A
 City: N/A
 State: N/A Zip Code: N/A

Investigation Request Status History

Created By: PS123.01 - JPAS/JCAVS Training for Security Professional, Level 2
 Reviewed By: PS123.01 - JPAS/JCAVS Training for Security Professional, Level 2
 Approved By: PS123.01 - JPAS/JCAVS Training for Security Professional, Level 2
 Approver Phone: (703) 465-1234

Status	Date
Pending PSI	2004 09 18
Initiated PSI	2004 09 19
Initiated PSI (Stopped)	2004 09 20
Initiated PSI (Resumed)	2004 09 21
Ready for Review PSQ	2004 09 22
Ready for Approval PSQ	2004 09 23
Approved PSQ	2004 09 23

[Close](#)

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

An example of *Investigation Request Status History* section on the Add/Modify Investigation Request screen is shown above.

If during the review you find errors or items that applicant needs to update, you can select **REVISE**. See **Revise** section for details

If during the review you determine that the applicant no longer needs the PSI, you can select **STOP**. See **Stop** Section for details.

Revise

If, during the review, you find errors or items that the applicant needs to update, you can select the **Revise PSQ** radio button.

1. On the Add/Modify Investigation Request screen, scroll down to the bottom of the page.
2. Select the **Revise PSQ** radio button and the **Revision Reason** box will appear.

Figure 43h “Add/Modify Investigation Request” with Investigation Request Status History screen (bottom) - Revision

Requesting Official

*Name: Captain John Smith
Title:
*Phone Number: (111) 222-3333 Extension:

Security Folder

*Location: At SOI
Location Name:
Street Address 1:
Street Address 2:
Street Address 3:
City:
State: Zip Code:

Official Personnel Folder

*Location: NPRC
Location Name:
Street Address 1:
Street Address 2:
Street Address 3:
City:
State: Zip Code:

Investigation Request Status History

Created By: PS123.01 - JPAS/JCAVS Training for Security Professional, Level 2

Status	Date
Pending PSI	2004 09 18
Initiated PSI	2004 09 19
Initiated PSI (Stopped)	2004 09 20
Initiated PSI (Resumed)	2004 09 21
Ready for Review PSQ	2004 09 22

[View PSQ](#) [View Signature Page](#)

☐ Review PSQ ☐ Review and Approve PSQ ☒ Revise PSQ ☐ Stop PSQ

Revision Reason:

3. Select the applicable **Revision Reason** from the drop down menu.
4. Click **Save** or **Save and Return**. (When you select **Save**, you remain on the page. If you select **Save and Return**, you return to the previous page.)
5. Applicant can now reenter e-Qip and update information.

Note: Notify the applicant to reenter e-QIP.


Remember: A reviewer/approver must review and/or approve the revised PSQ.

Stop

If during the review, you determine that the applicant no longer needs the PSI, you can select the **Stop PSQ** radio button.

1. On the Add/Modify Investigation Request screen, scroll down to the bottom of the page.
2. Select the **Stop PSQ** radio button and then click **Save**. Action is completed. Result: The *Investigation Request Status History* shows the Investigation Request as stopped (not shown in this screen capture).

Figure 43i: Add/Modify Investigation Request with Investigation Request Status History screen (bottom) - Stop



- Select Person
- View SMO
- Create/Modify Visit
- Notifications >
- Reports >
- Access Number
- PSM Net
- Home
- Manage Invest Rqsts >
 - Create Invest Rqst
 - Invest Rqst Status
- Chg Password
- Chg Category/Level
- Tutorial
- Tutorial
- Logout

Additional Scope Information

*Form Type: SF-86

*Date of Birth: 1966 01 25

Advance NAC Extra Coverage: No

*Local Agency Check Date: 2004 09 18

*Service Agency: Marines

SOI: NV00

*OPAC-ALC: DoD-MC

*Position Title: Military

*Access Code: SCI

Sensitivity ADP: IT-I

SON: N999

Additional Request Information

Requesting Official

*Name: Captain John Smith

Title: N/A

*Phone Number: (111) 222-3333

*Location: At SOI

Location Name: N/A

Street Address 1: N/A

Street Address 2: N/A

Street Address 3: N/A

City: N/A

State: N/A

Security Folder

Extension: N/A

Official Personnel Folder

*Location: NPRC

Location Name: N/A

Street Address 1: N/A

Street Address 2: N/A

Street Address 3: N/A

City: N/A

State: N/A

Investigation Request Status History

Created By: PS123.01 - JPAS/JCAVS Training for Security Professional, Level 2

Status	Date
Pending PSI	2004 09 18
Initiated PSI	2004 09 19

☐ Stop PSQ

Save

Save and Return

Cancel

Where do I mail release forms?

Mail the e-QIP releases and fingerprint cards to:

E-QIP Rapid Response Team
OPM-FIPC
PO Box 618
Boyers, PA 16018

Or

Ship via FedEx to:
E-QIP Rapid Response Team
OPM-FIPC
1137 Branchton Rd.
Boyers, PA 16018

Or

Fax Release forms (without fingerprint cards - recommended for PRs only) to:
724-794-1412
Attn: e-QIP Release Forms Processor

Or

E-mail scanned signature, release forms and Livescan Fingerprints to:

e-Qip.attachments@opm.gov

What about the Applicant?

One of the major conveniences of the e-QIP system is that it is web-based, so you can access the system from anywhere you have internet access, such as your home or office. Since e-QIP is a web-based system, it is important that you have your internet browser properly configured. The following guidance is provided for use by DoD requesters/users of e-QIP to help you properly configure your computer:

1. Start your internet browser and enter the following URL website address:

www.opm.gov/e-qip/

2. The e-QIP Gateway Page will appear. Scroll down and click the link labeled **e-QIP Applicant Site**.
3. A “browser checker” utility will automatically run and test your computer for e-QIP compatibility. Click the **Continue** button to proceed to the application. (If after doing so you receive the error message, *Page Cannot Be Displayed*, please ensure that you have properly configured your computer and that you have enabled TLS 1.0 (found under Internet Options). If you experience difficulty configuring your computer, try another computer or contact the DoD Security Services Center at 888-282-7682.)
4. A **Security Alert** box will appear, asking “**Do you want to proceed?**” If it does, click the Continue button .
5. The e-QIP **Login** Screen will appear. Enter your Social Security Number in the text entry boxes, and click the **Submit** button to logon to the e-QIP applicant site.
6. Initially you’ll be asked to answer three default “Golden Questions.” You will be required to type in your last name, the year when you were born and the city where you were born. IMPORTANT: Type “unknown” (case sensitive) for the answer to Question #3, “In what city were you born?” Then you may create new Golden Questions and Answers on the next screen.
7. Click the **Submit** button. The **Golden Questions** screen appears again prompting you to enter new Golden Questions. Enter new Golden Questions and Answers and then click **Submit**.
8. Click the **Enter Your Data** link.
9. Complete the SF-86 questions and save as instructed. Validation of your data will occur after every screen save.
10. Once you have completed the form, but BEFORE you certify your form, print out a copy of the PSQ.
11. At this point, local procedure will dictate your action prior to selecting the **Release Request/Transmit to Agency** link.

For additional information on using the e-QIP system and completing your PSQ, click on the **e-QIP Brochure for Applicants** located at the e-QIP Gateway <http://www.opm.gov/e-qip/> .

Section 14 – How to Generate a Request to Research/Upgrade Eligibility (RRU)

Introduction

The RRU is simply a direct notification to the appropriate CAF of any status changes a user cannot make within the system.

There are several reasons for which you would submit an RRU to the appropriate CAF. A RRU for personal information changes is only done if the person has an open investigation or they have an active DoD category – otherwise just make the changes locally(Industry).

The following are some examples of when you will submit an RRU for a person:

- *A person's eligibility level does not reflect the current investigation that was conducted by another investigative agency, e.g., the Air Force has a more current investigation than what DISCO has on file*
- *To downgrade a person's eligibility*
- *To correct a person's SSN*

*The main thing you have to remember before you attempt to send an RRU on a person is that **you must have an owning or servicing “relationship” with that person.** (Refer to Section 7 – “How to In-Process”)*

Instructions

1. Log in as a **User** of the appropriate SMO.
2. Click on **Select Person** (column on left).
3. Enter the person's **SSN**.
4. Click on the gray **Display** button.
5. The person's Personal Summary screen should appear with the person's name printed at the top. Make sure the category box located within the Personal Identification section is displaying the correct organization. If the correct organization is not being displayed, click on the drop down box and scroll down and highlight the correct organization.

NOTE: When the “Person Summary” screen first appears and you get an error message that says, *The Person Category does not have any Owning/Servicing Relationship and no Notification based on Owning/Servicing Relationship will be sent*, then the listed category is not currently in a PSM Net.

6. Once the proper category is listed and the person has an appropriate relationship with the SMO, the **Request to Research/Upgrade Eligibility** hyperlink will be present (Figure 36).

Figure 36: Personnel Summary screen

Person Summary

HARBACK, HELEN K
Person Category Industry (Contractor) HH3VFDDB
SSN: 926-60-5777

Open Investigation: N/A
PSQ Sent Date: N/A
Attestation Date: N/A
Incident Report: N/A
SF 713 Fin Consent Date: N/A
SF 714 Fin Disclosure Date: N/A
Polygraph: N/A
Foreign Relation: N/A

[PSQ Sent](#)
[Non-SCI Access History](#)
[Unofficial Foreign Travel](#)
[NdS History](#)

Date of Birth: 1966 05 17
Marital Status: N/A
Place of Birth: New York
Citizenship: U.S. Citizen
NdA Signed: Yes
NdS Signed: Yes

[SCI Access History](#)

[Request to Research/Upgrade Eligibility](#)
[NdA History](#)

Accesses

Category	US Access	PSP	Suitability and Trustworthiness	SCI	Available Actions
Industry (Contractor) HH3VFDDB	Top Secret	No	IT: N/A Public Trust: N/A Child Care: N/A	Access Number: N/A	Indoctrinate Non-SCI Debrief Non-SCI Indoctrinate SCI Request SPA
Industry (Contractor) 7N699-I		No	IT: N/A Public Trust: N/A Child Care: N/A	Access Number: N/A	
Industry (Contractor) 0S482-I	Top Secret	No	IT: N/A	SI	Indoctrinate Non-SCI

- Click on the **Request to Research/Upgrade Eligibility** hyperlink.
- The Request to Research/Recertify/Upgrade Eligibility screen should appear (Figure 37).

Figure 37: Request to Research/Recertify/Upgrade Eligibility screen

JCAVS Frameset - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media Print Mail News RSS Feeds

Address http://localhost:8085/JPAS/Training/Common/frame.jsp Go Links

Request to Research/Recertify/Upgrade Eligibility

BUGETT, BELINDA C.
SSN: 123453001

***UNCLASSIFIED** Justification: (Please include the Requestor's DSN/Commercial phone numbers)

***Please select one of the following Adjudication Types**

☐ Check to research this person's eligibility

☐ Check to recertify this person's current eligibility

☐ Check to upgrade this person's eligibility based on current investigation

***Select the CAF to receive the request**

SAVE CANCEL

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

Done Local intranet

Start

2:50 PM

9. In the **Justification** text box, enter details of the request along with your telephone number.
10. Click on **one** of the three **radio buttons** that are available. (4 radio buttons for Industry)
11. Click on the **Select the CAF to receive the request** drop down menu and select the appropriate CAF to which you want the RRU sent.
12. Click the gray **Save** button.

NOTE: Once you send an RRU on a person, you will not be able to submit another RRU until the first one has been answered by the CAF. Continue to check **Notifications** to see the status of the RRU.

Section 15 – How to Check Notifications

Introduction

*Notification is the means by which a CAF will contact you concerning any JPAS actions. For example, if there is a change to an employee's eligibility status or the CAF is responding back to an RRU, you will receive this via **Notifications**. You can only see notifications associated with your SMO.*

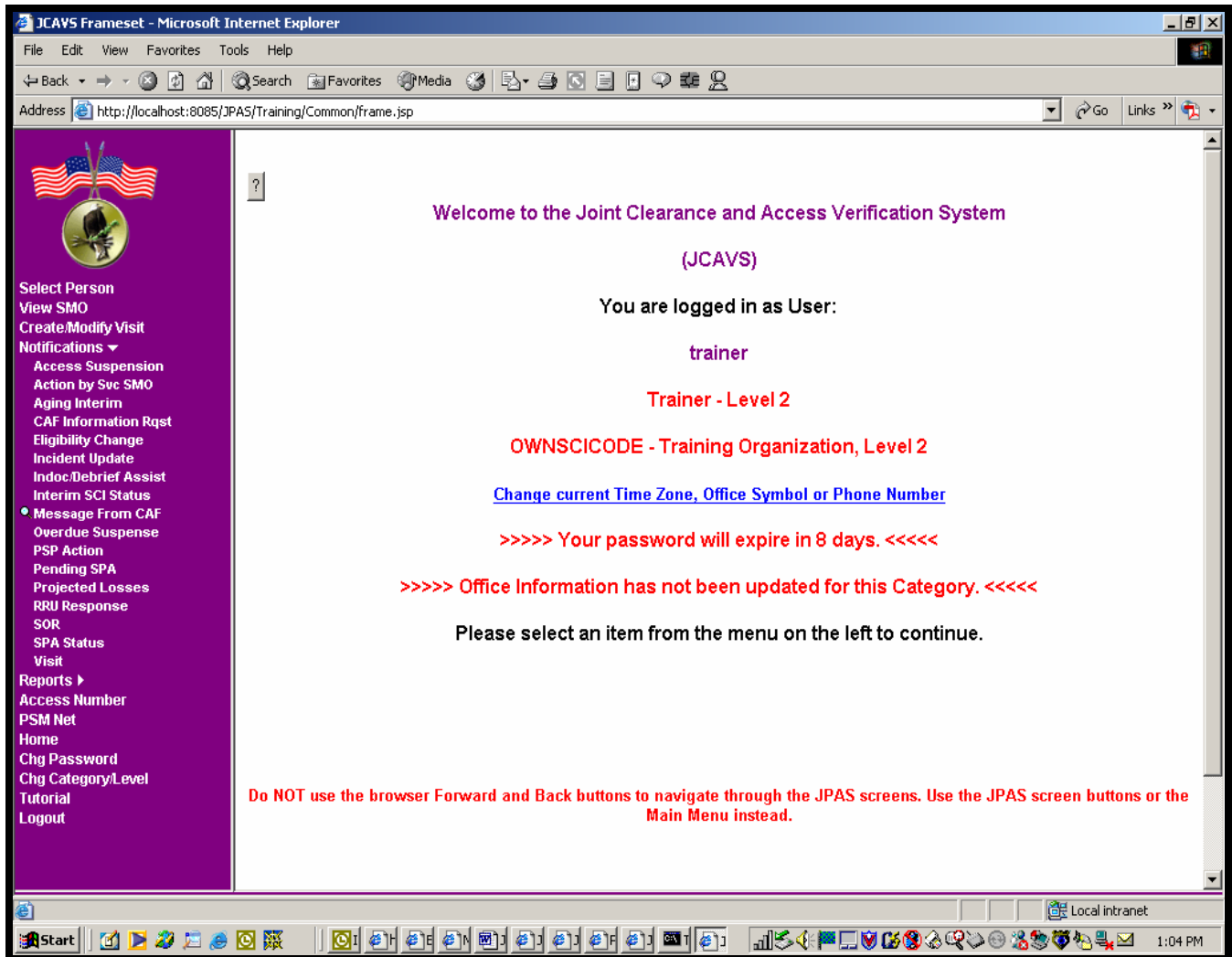
*You should check the notification menu at least once a week, but daily would be better. All notifications will remain present for 30 days or you can indicate immediate removal by checking the **Remove from Display** box and **Confirm**.*

You will know you have a notification if there is a “magnifying glass” immediately to the left of the Notifications list.

Instructions

1. Log in as a **User** for the SMO.
2. Click on **Notifications** (column on left).
3. The notification sub-menu will appear underneath the word **Notifications**.
4. If you have any notifications, you will see a magnifying glass immediately to the left of the sub-menu item (Figure 38).

Figure 38: Welcome screen showing notifications



5. If you click on the **notification that has a magnifying glass**, it will open a screen showing you the notification for that particular sub-menu item. The screen in Figure 39 shows notification of a message from the CAF regarding a Research/Recertify/Upgrade Eligibility Request.

Figure 39: CAF Response to Research/Recertify/Upgrade Eligibility Request Notification screen

CAF Response to Research/Recertify/Upgrade Eligibility Request Notification

SSN	Name	Request Type	CAF Response	Remove From Display
000-02-0754	BROWN, JOHN B	Upgrade Eligibility	unclassified comment	<input type="checkbox"/>
000-02-0753	COOPER, FRED F	Upgrade Eligibility	unclassified comment	<input type="checkbox"/>
000-02-0749	DODGE, MARY O	Research Eligibility	unclassified comment	<input type="checkbox"/>
000-02-0755	DODSON, PAUL G	Upgrade Eligibility	unclassified comment	<input type="checkbox"/>
000-02-0744	ELLIS, BILL C	Recertify Eligibility	unclassified comment	<input type="checkbox"/>
000-02-0745	ELLIS, ROBERT L	Recertify Eligibility	unclassified comment	<input type="checkbox"/>
000-02-0750	EVANS, SALLY S	Research Eligibility	unclassified comment	<input type="checkbox"/>
000-02-0756	HAMMER, ACE G	Upgrade Eligibility	unclassified comment	<input type="checkbox"/>
000-02-0757	KING, BEE K	Upgrade Eligibility	unclassified comment	<input type="checkbox"/>
000-02-0746	MARTIN, PAMELA S	Recertify Eligibility	unclassified comment	<input type="checkbox"/>
000-02-0741	MCCOY, DONNA U	Recertify Eligibility	unclassified comment	<input type="checkbox"/>
000-02-0748	MCCOY, DONNA U	Research Eligibility	unclassified comment	<input type="checkbox"/>
000-02-0747	MOORE, TROY Z	Research Eligibility	unclassified comment	<input type="checkbox"/>
000-02-0742	NEWMAN, CORY W	Recertify Eligibility	unclassified comment	<input type="checkbox"/>
000-02-0743	SHAFER, DAN A	Recertify Eligibility	unclassified comment	<input type="checkbox"/>
000-02-0751	SUNBURY, CLAIRE T	Research Eligibility	unclassified comment	<input type="checkbox"/>
000-02-0752	WALLS, LISA Y	Upgrade Eligibility	unclassified comment	<input type="checkbox"/>

Confirm

Cancel

Notice: Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

- The individual's SSN will be hyperlinked and if you click on the **SSN** it will take you to that individual's Person Summary screen.
- If you click the gray **Cancel** button it will take you back to the Main Menu.

Section 16 – How to Generate a Report

Introduction

*There are several different types of reports that can be generated from the **Report** menu within JCAVS.*

The Periodic Reinvestigation report will provide you with a customized printout of everyone that is within your SMO whose investigation is out-of-scope and requires a Periodic Reinvestigation.

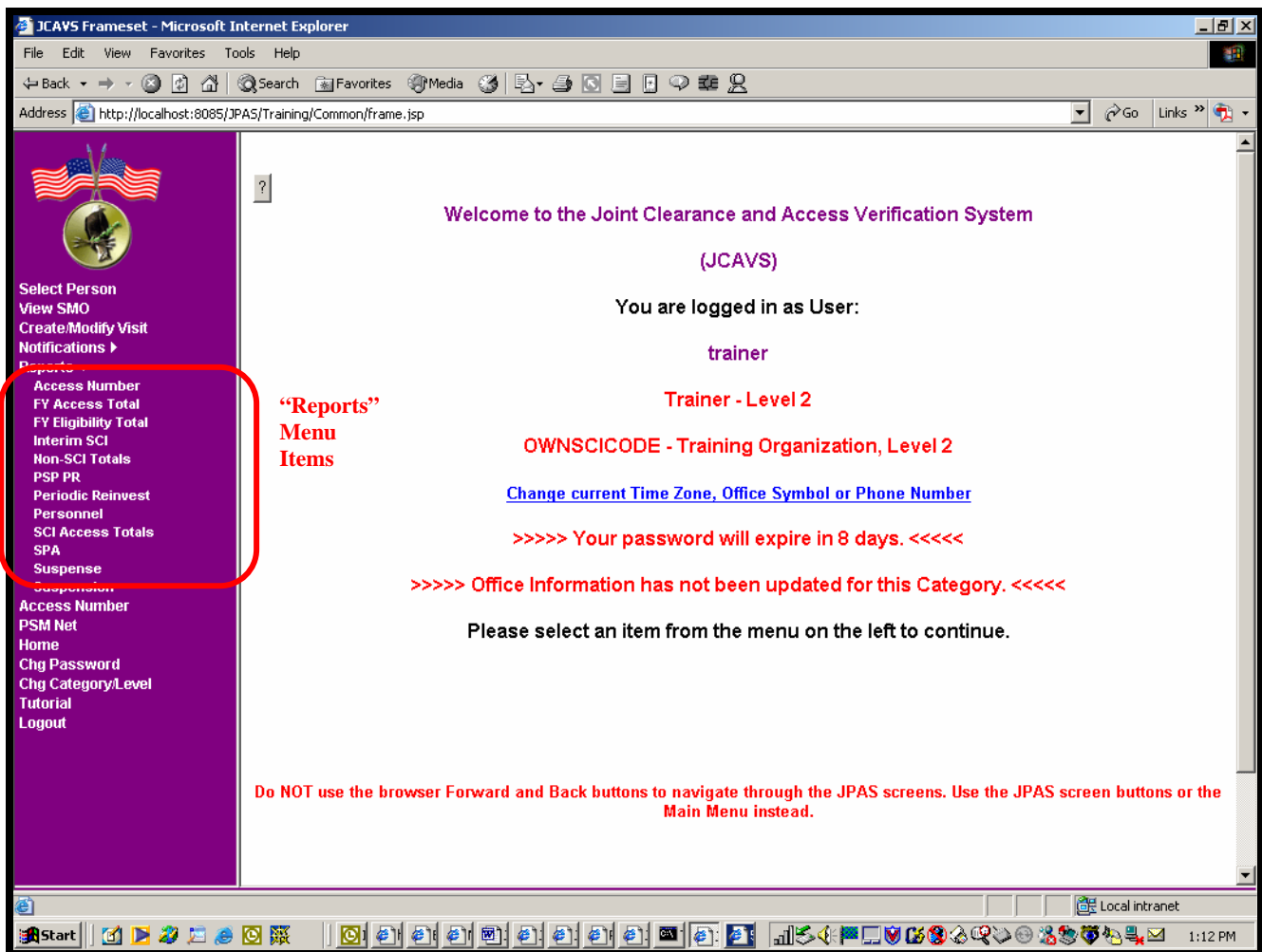
The Personnel report will provide you with a customized report containing your entire SMO sorted into different sections based on Organizations and the relationship of a person.

It is highly recommended that you use Internet Explorer when you want to generate a report. Reports can be produced in PDF or Excel format.

Instructions

1. Log in as a **User** for the SMO.
2. Click on **Reports** (column on left).
3. The sub-menu items will appear underneath the word **Reports**.

Figure 40: Welcome screen



4. Click in the **Reports** sub-menu, on the type of report you want to generate.
5. A new window will open which will allow you to customize your reports (Figure 41a).

Figure 41a: Personnel by Eligibility and Access Report screen

Personnel by Eligibility and Access Report

*** Report On:**
☒ My Office Only
☐ My Office and Immediate Subordinates
☐ My Office and all Subordinates

*** For Persons:**
☐ Owned Only
☐ Serviced Only
☒ Owned and Serviced

*** Organization:**
☒ All Organizations
☐ Organization's Service Agency:

*** Enter Search Criteria (include an * for wildcarding):**
Organization Name:
Organization Location:
Organization Code:

*** Eligibility:**

*** Investigation Type:**

*** Position Code:**

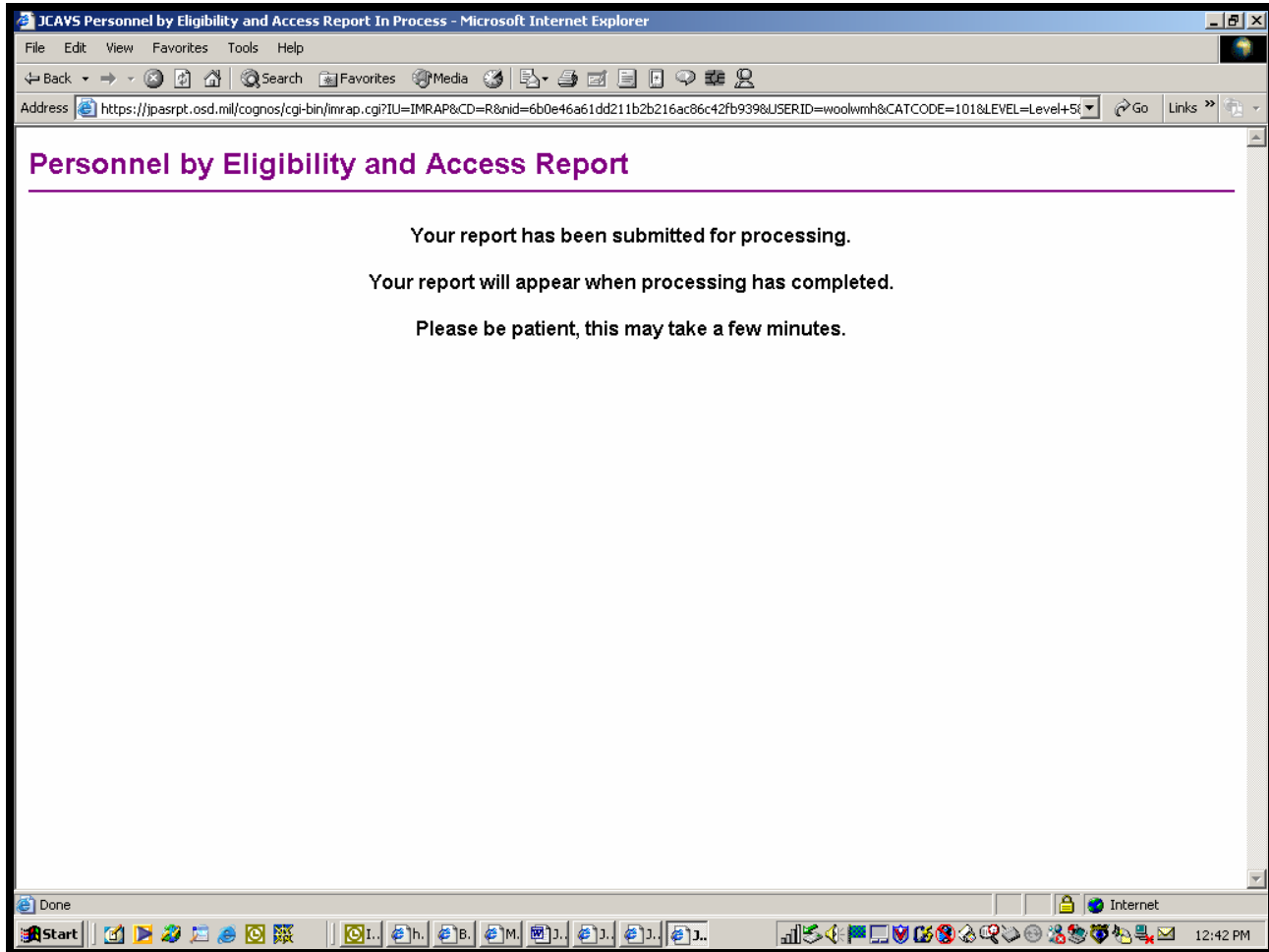
*** Position Sensitivity:**

*** Sort By:**
☒ Name
☐ SSN

Next >

6. Under the **Report On** section, the default is **My Office Only** with two other options concerning subordinates. The options with Subordinates apply only if you have established a “Parent/Child” relationship with other organizations. If you do not have any “Parent/Child” relationships established, use the default setting.
7. Under the **For Persons** section, the default is **Owned and Serviced** with two other options. You can either select the report to contain only records on persons with whom you have an “owning” relationship or a “servicing” relationship with the SMO. If you want both, then stay with the default setting.
8. There are six other sort filter drop down menus that you **must** populate before running the report. In most cases you will just populate them with **ALL** which is the first option available when you click on the drop down. You can, however, pick any of the other available options if you want to customize your report. If you sort by organization, the sort will be based on organizations in your PSM network.
9. Once you have made your choices, click on the gray **Run Report** button.

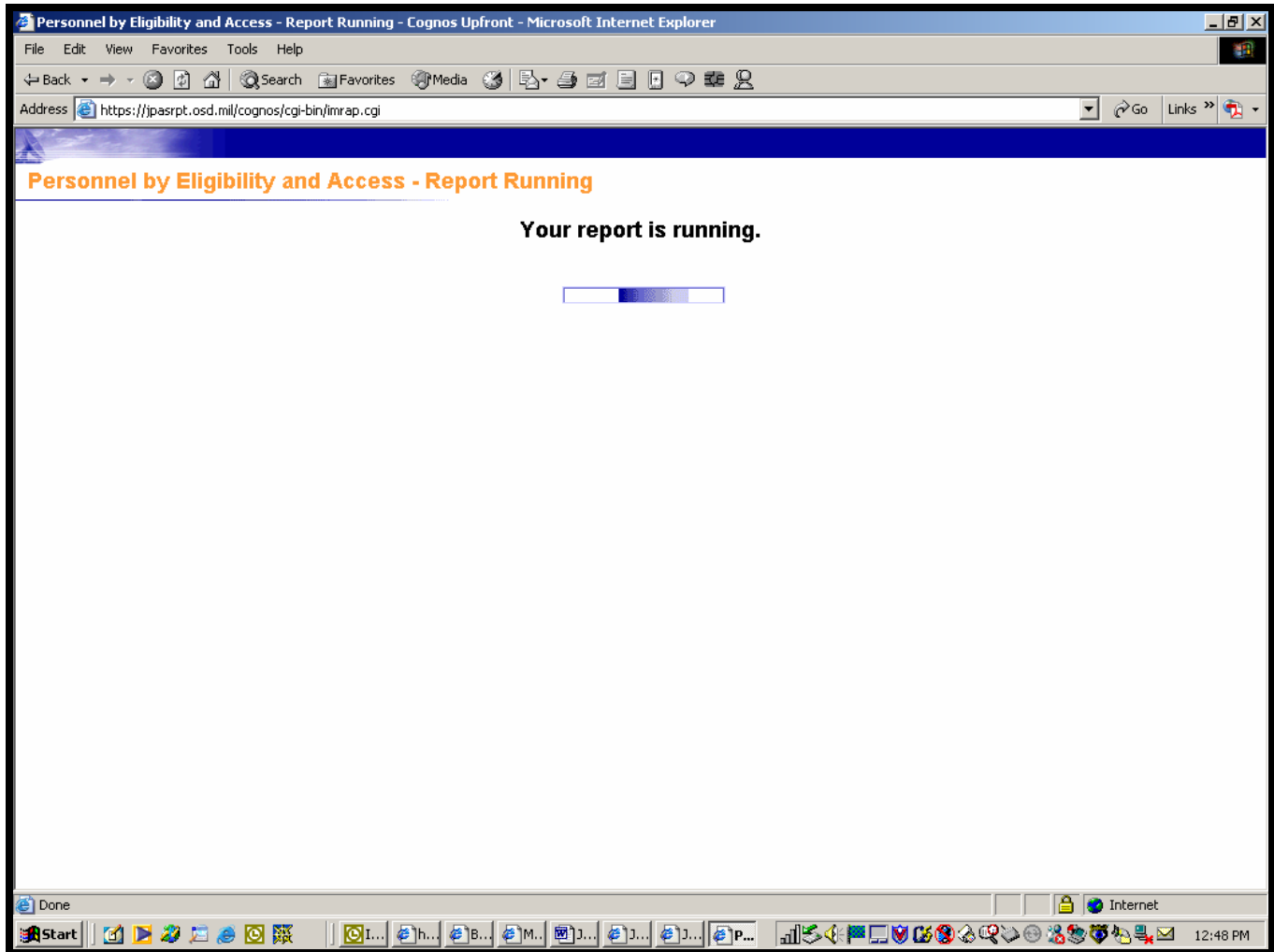
Figure 41b: Personnel by Eligibility and Access Report screen



10. You will then see a screen informing you that the report is being processed (Figure 41b). The report will appear once the processing has been completed.

11. While the report is processing, you will see the following screen indicating your report is running.

Figure 41c: Personnel by Eligibility and Access Report Running screen



Screen Print 13-4

12. After the report has finished processing, you will see the final report sorted according to the SSN of the person contained with each organization.

NOTE: On the bottom left of the screen you will see two icons. The icon on the left allows you to view the report as a PDF file. The icon on the right allows you to view the report as an Excel file.

Section 17 – Mass Personnel Changes (Industry)

Introduction

The “Manage Mass Personnel Changes” screen allows JAMS DISCO CAF Users (Manager, Supervisor or Adjudicator) or JCAVS Industry Users (Level 2 through 6) to perform transfers and/or separations on multiple Industry persons within a given organization.

Separate Only: Allows the user to separate all or some of the Person Categories in the Organization and debriefs all Non-SCI Accesses. This function would be used for events such as:

- Termination of a CAGE code or
- Reductions in force (layoffs)

Notification is sent to the DISCO CAF if person has an open Investigation.

Separate and Transfer Multiple Facility Organization (MFO): Allows the user to move all or some of the Person Categories to an Organization within home offices.

- Multiple Facility Transfers (MFT) within an MFO
 - Employee stays with the same company but transfers from one cleared organization to another cleared organization AND both organizations are in the same Multiple Facility Organization (with the same Home Office).

JPAS updates the Person Category Organization and creates a history of Organization and Access.

Notification is sent to the DISCO CAF if the person has an open Investigation.

Separate and Transfer Non-MFO: Allows a Security Officer to move all or some of the Person Categories to an Organization outside of the home offices.

- Multiple Facility Transfers (MFT) outside an MFO
 - Employee stays with the same company but transfers from one cleared organization to another cleared organization BUT the organizations are in different Multiple Facility Organizations (with different Home Offices).

JPAS updates the Person Category Organization and creates a history of Organization and Access. Non-SCI Access may be downgraded.

Notification is sent to the DISCO CAF if the person has an open Investigation.

Transfer Non-MFO: Allows the user to move all or some Person Categories to an Organization outside of home offices while retaining the current Organization. JPAS creates a new Person Category. This function would be used for events such as:

- Divestiture – When a portion of a company is sold and some of the employees are transferred to the new company.

The qualifying Non SCI Access is moved to the new Person Category

Notification is sent to the DISCO CAF if the person has an open Investigation

Instructions

1. Log in as a **User** for the SMO.
2. Click on **Mass Personnel** link.
3. The JPAS “Manage Mass Personnel Changes” screen displays (Figure 42a).
4. From the **Action** drop down menu, highlight and select the appropriate Action to be taken
5. From the **Separation Type** drop down menu, highlight and select the appropriate Separation Type.
6. Click on the **Losing Organization: Select Organization** button to display the JPAS “Organization Search” screen.
7. Select the appropriate losing organization from the JPAS “Organization Search” screen. The JPAS “Manage Personnel Changes” screen will refresh with the losing organization’s information.

Figure 42a: Manage Mass Personnel Changes screen

Manage Mass Personnel Changes - Microsoft Internet Explorer provided by EDS COE

File Edit View Favorites Tools Help

Manage Mass Personnel Changes

*Action: Separation and Transfer - MFO

Separation Type:

Losing Organization:

Name: LOCKHEED MARTIN
CORP,SPACE SYS

Organization Code: 06887-I

Location: SUNNYVALE

Clearance: Top Secret

Status: Active

Number of Person Categories: 264

Gaining Organization:

Name: LOCKHEED MARTIN
AERONAUTICS CO

Organization Code: 81755-I

Location: FORT WORTH

Clearance: Secret

Status: Active

Person Categories Attached to Losing Organization:

Records 1 - 50 of 237, Page 1 of 5

1 2 3 4 5 Next Last

Sort/Find By: ☒ Ascending ☐ Descending

Find:

SSN	Name	Eligibility	Non-SCI Access	Select
	ABUEG, ROLANDO	Top Secret	SIGMA 16	<input type="checkbox"/>
2138	AGURS, TRINA	Top Secret	Cosmic Top Secret (NATO)	<input type="checkbox"/>
8748	ALEXANDER, DERRICK	Top Secret	SIGMA 16	<input type="checkbox"/>
5302	BASS, DANIEL	Top Secret	SIOP-3	<input type="checkbox"/>
4269	BERGER, MICHAEL	Top Secret	Atomal Top Secret	<input type="checkbox"/>
0334	BERNARD, EDWARD	Top Secret	SIGMA 16	<input type="checkbox"/>
2085	BERRY, ELLSWORTH	Top Secret	Cosmic Top Secret (NATO)	<input type="checkbox"/>
0094	BETTERS, MARK	Top Secret	SIGMA 16	<input type="checkbox"/>
0000	BOLMAN, BOBNEY	Top Secret	SIGMA 16	<input type="checkbox"/>

8. Click on the **Gaining Organization: Select Organization** button to display the JPAS Organization Search screen.
9. Select the appropriate gaining organization from the JPAS Organization Search screen. The JPAS Manage Personnel Changes screen will refresh with the gaining organization's information.
10. Click on the **Display Eligible Personnel** button. The screen refreshes with selected Person Category records eligible for update (Figure 42a).
11. Click on the **Select All on Page** button (not shown in this figure) to select all persons listed or check the **Select** box to select persons individually.

Figure 42b: Manage Mass Personnel Changes screen

The screenshot shows a web browser window titled "Manage Mass Personnel Changes - Microsoft Internet Explorer provided by EDS COE". The browser's menu bar includes "File", "Edit", "View", "Favorites", "Tools", and "Help". The main content area has a purple header "Manage Mass Personnel Changes" with a question mark icon. Below the header, there are two dropdown menus: "*Action:" set to "Separation Only" and "Separation Type:" set to "Separation".

Below these are two columns of organization information:

Losing Organization: <input type="button" value="Select Organization"/>	Gaining Organization: <input type="button" value="Select Organization"/>
Name: LOCKHEED MARTIN CORP,SPACE SYS	Name: N/A
Organization Code: 06887-I	Organization Code: N/A
Location: SUNNYVALE	Location: N/A
Clearance: Top Secret	Clearance: N/A
Status: Active	Status: N/A
Number of Person Categories: 27	

Below the organization information is a section titled "Person Categories Attached to Losing Organization:" with two buttons: "Display Eligible Personnel" and "Display Ineligible Personnel".

A warning message states: "WARNING: Processing more than 500 Person Categories may result in a long wait period. Please wait for your request to be processed." Below this are three buttons: "Save", "Save Entire Organization", and "Cancel".

At the bottom, a red "Notice:" states: "Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives."

12. Click on the **Save** button to update the selected records shown on this screen.
13. Click on the **Save Entire Organization** button to update the entire organization's records.
14. Click on the **Cancel** button to abandon changes made on this screen.

Section 18 - Terms and Definitions

- ***Collateral:*** Access to information identified as National Security Information that is not subject to enhanced security protection required for Special Access Program (SAP) information.
- ***Debrief:*** To remove an access level; requires debrief date and reason for debrief.
- ***Indoctrinate:*** To assign an access level to a cleared employee once they have a completed investigation or interim approval.
- ***In-Process:*** To enter person into your PSM Net.
- ***Notifications:*** The means by which you will be notified of any JPAS actions indicated on the JPAS Welcome Screen by a magnifying glass just to the left of the Notifications sub-menu item.
- ***Organization:*** An Organization is a unique code that has been assigned for each CAGE (Industry) and UIC (DoD) within the JPAS system. The Organization's identifier for Industry contains the CAGE code immediately followed by a hyphenated "I." For example, CAGE "1D020" would be established as "1D020-I." Each person within JPAS must be assigned to an organization.
- ***Out-Process:*** To remove a person no longer assigned to your SMO.
- ***Owning/Servicing:*** When adding someone to your SMO, you must determine if you want to "own" them or just "service" them. The easiest way to determine if you should own or service a person is to ask the question, "Who is responsible for updating this person's security clearance?" If you are responsible, then you should "own" this person.
- ***Personnel Security Management Network (PSM Net):*** A PSM Net is a listing of everyone within your SMO (listed by SSN) for whom YOU are responsible for maintaining/updating their security clearance information.
- ***Security Management Office (SMO):*** A SMO is established by an FSO and can contain one or more Organization. Each FSO must determine the number of Organizations they want within their SMO. For example, if an FSO has four (4) different Organizations, the FSO could either establish a separate SMO for each Organization or establish one SMO for all four Organizations. The SMO is responsible for "maintaining" the clearances for everyone "owned" within the SMO.

Section 19 - Acronyms

AM	Account Manager
ANACI	Access National Agency Check with Written Inquires
CAF	Central Adjudicating Facility
CAGE	Commercial and Government Entity Code
CC	Chain of Command
CNWDI	Critical Nuclear Weapons Design Information
DEERS	Defense Enrollment Eligibility Reporting System
DepSecDef	Deputy Secretary of Defense
DISCO	Defense Industrial Security Clearance Office
DoD	Department of Defense
DoE	Department of Energy
EPSQ	Electronic Personnel Security Questionnaire
e-QIP	Electronic Questionnaire for Investigation Processing
FSO	Facility Security Officer
ISL	Industrial Security Letter
JCAVS	Joint Central Adjudication & Verification System
JPAS	Joint Personnel Adjudication System
KMP	Key Management Personnel
LOC	Letter of Consent
NAC	National Agency Check
NACLAC	National Agency Check with Local Area Check
NACLC	National Agency Check with Local Area Check and Credit Check
NATO	North Atlantic Treaty Organization
NdA	Non-disclosure Agreement (Non-SCI/DoD)
NdS	Non-disclosure Statement (SCI)
NLC	National Agency Check with Local Area Check and Credit Check
NRO	National Reconnaissance Office
PASCODE	Personnel Accounting System Code
PCS	Permanent Change of Station
PR	Periodic Reinvestigation

PSM Net	Personnel Security Management Network
RRU	Request for Research/Recertify/Upgrade Eligibility
RUC	Reporting Unit Code
SAP	Special Access Program
SCI	Sensitive Compartmented Information
SIGMA 16	Reserved for DoE
SII	Special Investigative Inquiry
SIOP	Single Integrated Operating Plan
SMO	Security Management Office
SPA	Special Purpose Access
SOR	Statement of Reason
SSBI	Single Scope Background Investigation
SSN	Social Security Number
SVC	Servicing
TDY	Temporary Duty
UIC	Unit Identification Code
VAL	Visit Authorization Letter
XNAC	Extended National Agency Check

Section 20 – Index of Figures

Figure 1: JPAS Gateway Home Page	6
Figure 2: JPAS Disclosure Screen	7
Figure 3: JPAS Log In screen	8
Figure 4: Choose Category/Level screen	10
Figure 5: JCAVS Welcome screen and Main Menu	11
Figure 6: Change Office Symbol/Telephone Number/Time Zone screen	12
Figure 7: Select Person screen	14
Figure 8: Person Summary screen	15
Figure 9: Security Management Office Search screen	17
Figure 10: Security Management Office Maintenance screen	18
Figure 11: Security Management Office Parent Maintenance screen	19
Figure 12a: Add/Modify/Remove JCAVS User screen (top)	21
Figure 12b: Add/Modify/Remove JCAVS User screen (bottom)	22
Figure 13: Change Password screen	25
Figure 14: Add/Modify/Remove JCAVS User screen showing Reset User Password	26
Figure 15: JCAVS Maintain PSM Net screen	28
Figure 16a: Organization Search screen	30
Figure 16b: Organization Search screen (populated)	31
Figure 17a: PSM Net Add Organization Person Categories screen	32

Figure 17b: PSM Net Add Organization Person Categories screens (results)	33
Figure 18: Add/Modify Non-DoD Person screen	35
Figure 19a: Organization Search screen	37
Figure 19b: Organization Search screen (results)	38
Figure 20: Add/Modify Non-DoD Person screen (bottom)	39
Figure 21: View/Modify In/Out screen	41
Figure 22: Person Summary (accesses) screen.	43
Figure 23a: Indoctrinate Non-SCI Access screen	44
Figure 23b: Indoctrinate Non-SCI Access screen	45
Figure 24a: Person Summary screen	46
Figure 24b: Person Summary screen	47
Figure 25a: Indoctrinate SCI Access screen	48
Figure 25b: Indoctrinate SCI Access screen	49
Figure 26: Person Summary (accesses) screen	51
Figure 27: Debrief Non-SCI Access screen.	52
Figure 28: Person Summary (accesses) screen	54
Figure 29: Debrief SCI Access screen	55
Figure 30: Person Summary screen	57
Figure 31: View/Modify In/Out screen	58

Figure 32: JCAVS Maintain PSM Net screen	59
Figure 33a: Add/Modify Non-DoD Person screen	62
Figure 33b: Add/Modify Non-DoD Person screen	63
Figure 34: Personnel Summary screen	64
Figure 35: PSQ/SF 86 Sent screen	65
Figure 12b: Add/Modify/Remove JCAVS Users screen (bottom)	67
Figure 5: JCAVS Welcome screen and Main Menu	69
Figure 7: Select Person screen	70
Figure 8a: Person Summary screen (middle)	70
Figure 43: Determine Investigation Scope screen	71
Figure 43a: Determine Investigation Scope Initiation Scope screen	72
Figure 43b: Add/Modify Investigation Request screen	72
Figure 43c: Add/Modify Investigation Request screen (bottom)	73
Figure 5: JCAVS Welcome screen and Main Menu	77
Figure 44: JCAVS Investigation Request Status Notification screen and Main Menu	77
Figure 43d: Add/Modify Investigation Request with Investigation Request Status History screen (bottom)	78
Figure 43e: Add/Modify Investigation Request with Investigation Request Status History screen (bottom) Industry	79
Figure 43f: Add/Modify Investigation Request with Investigation Request Status History screen (bottom) Approver	80

Figure 43g: Add/Modify Investigation Request with Investigation Request Status History screen (bottom) Approved	81
Figure 43h: Add/Modify Investigation Request with Investigation Request Status History screen (bottom) Revision.	82
Figure 43i: Add/Modify Investigation Request with Investigation Request Status History screen (bottom) Stop	83
Figure 36: Personnel Summary screen	87
Figure 37: Request to Research/Recertify/Upgrade Eligibility screen	88
Figure 38: JCAVS Welcome screen showing Notifications	90
Figure 39: CAF Response to Research/Recertify/Upgrade Eligibility Request Notification screen	91
Figure 40: JCAVS Welcome screen showing Reports	93
Figure 41a: Personnel by Eligibility and Access Report screen	94
Figure 41b: Personnel by Eligibility and Access Report screen	95
Figure 41c: Personnel by Eligibility and Access Report Running screen showing report running	96
Figure 42a: Manage Mass Personnel Changes screen	99
Figure 42b: Manage Mass Personnel Changes screen	100